

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-259214

(P2002-259214A)

(43) 公開日 平成14年9月13日 (2002.9.13)

| (51) Int.Cl. ⁷ | 識別記号 | F I | テ-マコ-ド*(参考) |
|---------------------------|-------|---------------|-------------------|
| G 0 6 F 12/14 | 3 1 0 | G 0 6 F 12/14 | 3 1 0 K 5 B 0 1 7 |
| 3/06 | 3 0 4 | 3/06 | 3 0 4 H 5 B 0 6 5 |
| | | | 3 0 4 F |

審査請求 未請求 請求項の数120 O L (全 24 頁)

(21) 出願番号 特願2001-31194(P2001-31194)

(22) 出願日 平成13年2月7日(2001.2.7)

(31) 優先権主張番号 60/180632

(32) 優先日 平成12年2月7日(2000.2.7)

(33) 優先権主張国 米国 (U S)

(31) 優先権主張番号 09/533009

(32) 優先日 平成12年3月22日(2000.3.22)

(33) 優先権主張国 米国 (U S)

(31) 優先権主張番号 09/604592

(32) 優先日 平成12年6月27日(2000.6.27)

(33) 優先権主張国 米国 (U S)

(71) 出願人 500503540

イーエムシー コーポレイション

アメリカ合衆国 マサチューセッツ

01748 ホプキントン パークウッド ド

ライヴ 35

(72) 発明者 ジェレミー・オヘア

アメリカ合衆国 マサチューセッツ

01748 ホプキントン ロッキー ウッズ

ロード 22

(74) 代理人 100077827

弁理士 鈴木 弘男

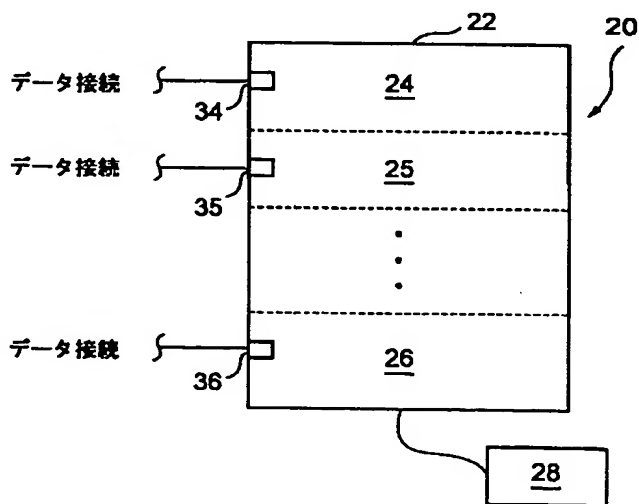
最終頁に続く

(54) 【発明の名称】 記憶装置へのアクセスの制御

(57) 【要約】 (修正有)

【課題】 データ記憶装置への制御システムコールアクセス方法および装置を提供する。

【解決手段】 複数のグループを規定し、各グループについて、複数のアクションタイプと、対応する許可レベルとを規定する。アクションタイプのサブセットについては、対応するアクションを実行する複数の装置を規定することであって、少なくともいくつかの装置はデータ記憶装置22の部分に対応し、少なくとも1つのグループについて、要求されたアクションについての許可を決定する。アクションが装置の1つに対応する場合は、少なくとも1つのグループに対応するアクションタイプについて許可レベルを調べることで、および要求されたアクションに対応する複数の装置を調べることでより許可が決定され、アクションが装置の1つに対応しない場合は、少なくとも1つのグループに対応するアクションタイプについての許可レベルを調べることでより許可が決定される。



【特許請求の範囲】

【請求項1】 アクションの許可を決定する方法において、
複数のグループを規定するステップと、
各グループについて、複数のアクションタイプと、対応する許可レベルとを規定するステップと、
少なくともアクションタイプのサブセットについて、対応するアクションを実行する複数の装置を規定するステップであって、少なくともいくつかの装置はデータ記憶装置の部分に対応するステップと、
少なくとも1つのグループについて、要求されたアクションについての許可を決定するステップと、を有し、
アクションが装置の1つに対応する場合に、前記少なくとも1つのグループに対応するアクションタイプについて許可レベルを調べることで、および要求されたアクションに対応する複数の装置を調べることでより許可が決定され、アクションが装置の1つに対応しない場合に、前記少なくとも1つのグループに対応するアクションタイプについての許可レベルを調べることでより許可が決定される方法。

【請求項2】 アクションタイプはデータ記憶装置へのシステムコールを含む請求項1に記載の方法。

【請求項3】 少なくとも1つの装置は、データ記憶装置の少なくとも1つのディスク記憶領域を含む請求項1に記載の方法。

【請求項4】 少なくとも1つの装置は、データ記憶装置の通信ポートを含む請求項1に記載の方法。

【請求項5】 アクションタイプは、システムコールが通信ポート上で許可されるか否かを示す請求項4に記載の方法。

【請求項6】 許可されている要求されたアクションに対して、アクションを実行する後続の要求に関して使用可能なタグを返すステップを有する請求項1に記載の方法。

【請求項7】 アクションに対する許可を決定する方法において、
要求者が要求者リストに含まれるか否かを決定するステップと、
要求されたアクションが要求者に関連するアクションタイプのリスト中に含まれるか否かを決定するステップと、
アクションが少なくとも1つの装置を使用する場合に、少なくとも1つの装置が要求者及び要求されたアクションに関連する装置リスト中に含まれるか否かを決定するステップと、を有し、装置リストはデータ記憶装置に関連する少なくともいくつかの装置を含む方法。

【請求項8】 要求者が要求者リスト中に含まれない場合、要求者リストからデフォルト要求者を使用するステップを有する請求項7に記載の方法。

【請求項9】 要求者が要求者リストに含まれない場合

に、許可を否定するステップを有する請求項7に記載の方法。

【請求項10】 要求されたアクションが少なくとも1つの装置を使用しない場合、要求されたアクションが要求者に関連付けされたアクションタイプのリストに含まれる場合にアクションを許可する請求項7に記載の方法。

【請求項11】 アクションタイプの少なくともいくつかはデータ記憶装置上で実行されるアクションに対応しない請求項7に記載の方法。

【請求項12】 アクションタイプはデータ記憶装置へのシステムコールを含む請求項7に記載の方法。

【請求項13】 少なくとも1つの装置は、データ記憶装置の少なくとも1つのディスク記憶領域を含む請求項7に記載の方法。

【請求項14】 少なくとも1つの装置は、データ記憶装置の通信ポートを含む請求項7に記載の方法。

【請求項15】 アクションタイプは、通信ポート上でシステムコールが許可されるか否かを示す請求項14に記載の方法。

【請求項16】 許可されている要求されたアクションに対して、アクションを実行する後続の要求に関連して使用可能なタグを返すステップを有する請求項7に記載の方法。

【請求項17】 アクションの許可を決定する装置において、

複数のグループを規定する手段と、
各グループについて、複数のアクションタイプと、対応する許可レベルとを規定する手段と、
少なくともアクションタイプのサブセットについて、対応するアクションを実行する複数の装置を規定する手段であって、少なくともいくつかの装置はデータ記憶装置の部分に対応する手段と、
少なくとも1つのグループについて、要求されたアクションについての許可を決定する手段と、を有し、
アクションが装置の1つに対応する場合に、前記少なくとも1つのグループに対応するアクションタイプについて許可レベルを調べることで、および要求されたアクションに対応する複数の装置を調べることでより許可が決定され、アクションが装置の1つに対応しない場合に、前記少なくとも1つのグループに対応するアクションタイプについての許可レベルを調べることでより許可が決定される装置。

【請求項18】 アクションタイプはデータ記憶装置へのシステムコールを含む請求項17に記載の装置。

【請求項19】 少なくとも1つの装置は、データ記憶装置の少なくとも1つのディスク記憶領域を含む請求項17に記載の装置。

【請求項20】 少なくとも1つの装置は、データ記憶装置の通信ポートを含む請求項17に記載の装置。

【請求項 2 1】 アクションタイプは、システムコールが通信ポート上で許可されるか否かを示す請求項 2 0 に記載の装置。

【請求項 2 2】 許可されている要求されたアクションに対して、アクションを実行する後続の要求に関して使用可能なタグを返す手段を有する請求項 1 7 に記載の装置。

【請求項 2 3】 アクションに対する許可を決定する装置において、
要求者が要求者リストに含まれるか否かを決定する手段と、
要求されたアクションが要求者に関連するアクションタイプのリスト中に含まれるか否かを決定する手段と、
アクションが少なくとも 1 つの装置を使用する場合に、少なくとも 1 つの装置が要求者及び要求されたアクションに関連する装置リスト中に含まれるか否かを決定する手段と、を有し、装置リストはデータ記憶装置に関連する少なくともいくつかの装置を含む装置。

【請求項 2 4】 要求者が要求者リスト中に含まれない場合、要求者リストからデフォルト要求者を使用する手段ステップを有する請求項 2 3 に記載の装置。

【請求項 2 5】 要求者が要求者リストに含まれない場合に、許可を否定する手段を有する請求項 2 3 に記載の装置。

【請求項 2 6】 要求されたアクションが少なくとも 1 つの装置を使用しない場合、要求されたアクションが要求者に関連付けされたアクションタイプのリストに含まれる場合にアクションを許可する請求項 2 3 に記載の装置。

【請求項 2 7】 アクションタイプの少なくともいくつかはデータ記憶装置上で実行されるアクションに対応しない請求項 2 3 に記載の装置。

【請求項 2 8】 アクションタイプはデータ記憶装置へのシステムコールを含む請求項 2 3 に記載の装置。

【請求項 2 9】 少なくとも 1 つの装置は、データ記憶装置の少なくとも 1 つのディスク記憶領域を含む請求項 2 3 に記載の装置。

【請求項 3 0】 少なくとも 1 つの装置は、データ記憶装置の通信ポートを含む請求項 2 3 に記載の装置。

【請求項 3 1】 アクションタイプは、通信ポート上でシステムコールが許可されるか否かを示す請求項 3 0 に記載の装置。

【請求項 3 2】 許可されている要求されたアクションに対して、アクションを実行する後続の要求に関連して使用可能なタグを返す手段を有する請求項 2 3 に記載の装置。

【請求項 3 3】 アクションの許可を決定するコンピュータソフトウェアにおいて、
複数のグループを規定する実行可能なコードと、
各グループについて、複数のアクションタイプと、対応

する許可レベルとを規定する実行可能なコードと、
少なくともアクションタイプのサブセットについて、対応するアクションを実行する複数の装置を規定する実行可能なコードであって、少なくともいくつかの装置はデータ記憶装置の部分に対応する実行可能なコードと、
少なくとも 1 つのグループについて、要求されたアクションについての許可を決定する実行可能なコードと、を有し、

アクションが装置の 1 つに対応する場合に、前記少なくとも 1 つのグループに対応するアクションタイプについて許可レベルを調べることで、および要求されたアクションに対応する複数の装置を調べることで許可が決定され、アクションが装置の 1 つに対応しない場合に、前記少なくとも 1 つのグループに対応するアクションタイプについての許可レベルを調べることで許可が決定されるコンピュータソフトウェア。

【請求項 3 4】 アクションタイプはデータ記憶装置へのシステムコールを含む請求項 3 3 に記載のコンピュータソフトウェア。

【請求項 3 5】 少なくとも 1 つの装置は、データ記憶装置の少なくとも 1 つのディスク記憶領域を含む請求項 3 3 に記載のコンピュータソフトウェア。

【請求項 3 6】 少なくとも 1 つの装置は、データ記憶装置の通信ポートを含む請求項 3 3 に記載のコンピュータソフトウェア。

【請求項 3 7】 アクションタイプは、システムコールが通信ポート上で許可されるか否かを示す請求項 3 6 に記載のコンピュータソフトウェア。

【請求項 3 8】 許可されている要求されたアクションに対して、アクションを実行する後続の要求に関して使用可能なタグを返す実行可能なコードを有する請求項 3 3 に記載のコンピュータソフトウェア。

【請求項 3 9】 アクションに対する許可を決定するコンピュータソフトウェアにおいて、
要求者が要求者リストに含まれるか否かを決定する実行可能なコードと、

要求されたアクションが要求者に関連するアクションタイプのリスト中に含まれるか否かを決定する実行可能なコードと、

アクションが少なくとも 1 つの装置を使用する場合に、少なくとも 1 つの装置が要求者及び要求されたアクションに関連する装置リスト中に含まれるか否かを決定する実行可能なコードと、を有し、装置リストはデータ記憶装置に関連する少なくともいくつかの装置を含むコンピュータソフトウェア。

【請求項 4 0】 要求者が要求者リスト中に含まれない場合、要求者リストからデフォルト要求者を使用する実行可能なコードを有する請求項 3 9 に記載のコンピュータソフトウェア。

【請求項 4 1】 要求者が要求者リストに含まれない場

合に、許可を否定する実行可能なコードを有する請求項39に記載のコンピュータソフトウェア。

【請求項42】 要求されたアクションが少なくとも1つの装置を使用しない場合、要求されたアクションが要求者に関連付けられたアクションタイプのリストに含まれる場合にアクションを許可する請求項39に記載のコンピュータソフトウェア。

【請求項43】 アクションタイプの少なくともいくつかはデータ記憶装置上で実行されるアクションに対応しない請求項39に記載のコンピュータソフトウェア。

【請求項44】 アクションタイプはデータ記憶装置へのシステムコールを含む請求項39に記載のコンピュータソフトウェア。

【請求項45】 少なくとも1つの装置は、データ記憶装置の少なくとも1つのディスク記憶領域を含む請求項39に記載のコンピュータソフトウェア。

【請求項46】 少なくとも1つの装置は、データ記憶装置の通信ポートを含む請求項39に記載のコンピュータソフトウェア。

【請求項47】 アクションタイプは、通信ポート上でシステムコールが許可されるか否かを示す請求項46に記載のコンピュータソフトウェア。

【請求項48】 許可されている要求されたアクションに対して、アクションを実行する後続の要求に関連して使用可能なタグを返す実行可能なコードを有する請求項39に記載のコンピュータソフトウェア。

【請求項49】 記憶装置へのアクセスを制限する方法において、記憶装置に設けられた複数のポートのうちの1つにより複数のホストシステムの各々を記憶装置へ接続するステップと、各ポートについて、システムコールが許容されるか否かを選択的に決定するステップと、を有し、システムコールが許容されないポートについては、そのポートに接続されたホストシステムによるシステムコールが記憶装置に、システムコールが実行されなかったことを示させる方法。

【請求項50】 ポートがシステムコールを受け入れ可能か否かを制御するメカニズムを設けるステップを有する請求項49に記載の方法。

【請求項51】 前記メカニズムを設けるステップは、記憶装置に接続された外部制御装置を設けることを含む請求項50に記載の方法。

【請求項52】 外部制御装置は、記憶装置へキャラクタを送信し、記憶装置からキャラクタを受信するダムターミナルのように動作する請求項51に記載の方法。

【請求項53】 システムコールを許容しないポート上でシステムコールを許容するオーバーライドメカニズムを設けるステップを有する請求項49に記載の方法。

【請求項54】 オーバーライドメカニズムはまた、シ

ステムコールを許容するポート上のシステムコールを阻止する請求項53に記載の方法。

【請求項55】 前記メカニズムが設定されてから所定時間量が経過した後にオーバーライドメカニズムをリセットするステップを有する請求項54に記載の方法。

【請求項56】 所定時間量は30分である請求項55に記載の方法。

【請求項57】 オーバーライドメカニズムの設定を容易にする外部制御装置を設けるステップを有する請求項53に記載の方法。

【請求項58】 外部制御装置を設けるステップは、記憶装置へキャラクタを送信し、記憶装置からキャラクタを受信するダムターミナルを設けることを含む請求項57に記載の方法。

【請求項59】 記憶装置の制御装置において、記憶装置にアクセスする少なくとも1つのグループを規定する手段と、記憶装置の装置のプールの少なくとも1つを規定する手段と、

複数のアクセスタイプを規定する手段と、少なくとも1つのアクセスタイプについて、前記少なくとも1つのグループによる前記少なくとも1つのプールへのアクセス権を決定する手段と、を備える装置。

【請求項60】 アクセスタイプは、システムコールを含む請求項59に記載の装置。

【請求項61】 前記少なくとも1つのグループおよび前記少なくとも1つのプールは、論理的ユニットおよび物理的ユニットのうちの少なくとも1つを含む請求項59に記載の装置。

【請求項62】 前記少なくとも1つのプールは、記憶装置の通信ポートを含む請求項59に記載の装置。

【請求項63】 アクセス権は、通信ポート上でシステムコールが許容されるか否かを示す請求項62に記載の装置。

【請求項64】 記憶装置へのアクセスを制限する装置において、

記憶装置について設けられた複数のポートのうちの1つにより、複数のホストシステムの各々を記憶装置へ接続する手段と、

各ポートについて、システムコールが許容されるか否かを選択的に決定するステップと、を有し、システムコールが許容されないポートについては、そのポートに接続されたホストシステムによるシステムコールが記憶装置に、システムコールが実行されなかったことを示させる装置。

【請求項65】 ポートがシステムコールを受け入れ可能か否かを制御するメカニズムを設ける手段を有する請求項64に記載の装置。

【請求項66】 前記メカニズムを設けるステップは、記憶装置に接続された外部制御装置を含む請求項50に

記載の方法。

【請求項67】 外部制御装置は、記憶装置へキャラクタを送信し、記憶装置からキャラクタを受信するダムターミナルのように動作する請求項66に記載の装置。

【請求項68】 システムコールを許容しないポート上でシステムコールを許容するオーバーライドメカニズムを有する請求項64に記載の方法。

【請求項69】 オーバーライドメカニズムはまた、システムコールを許容するポート上のシステムコールを阻止する請求項68に記載の装置。

【請求項70】 前記メカニズムが設定されてから所定時間量が経過した後にオーバーライドメカニズムをリセットする手段を有する請求項69に記載の装置。

【請求項71】 所定時間量は30分である請求項70に記載の装置。

【請求項72】 オーバーライドメカニズムの設定を容易にする外部制御装置を有する請求項69に記載の装置。

【請求項73】 外部制御装置は、記憶装置へキャラクタを送信し、記憶装置からキャラクタを受信するダムターミナルを含む請求項57に記載の方法。

【請求項74】 記憶装置のポートにおいて、記憶装置へ提供されるデータを受信する手段と、記憶装置からデータを送信する手段と、ポートへ提供されるシステムコールを禁止する手段と、を有し、システムコールは、データを送信または受信しない記憶装置のための管理動作の要求を含むポート。

【請求項75】 記憶装置上のポートを制御するコンピュータソフトウェアにおいて、記憶装置と通信する手段と、前記通信する手段に接続され、ポートが提供されたシステムコマンドを受け入れないようにさせるコマンドを記憶装置へ提供する制御手段と、を有し、システムコマンドは、記憶装置による管理動作の要求を含むソフトウェア。

【請求項76】 記憶装置のポートを制御する装置において、ポートに接続され、記憶装置とのデータ通信を処理するポートドライバと、ポートドライバに接続され、セキュリティ構成データ要素とオーバーライド表示データ要素に基づいて、ポートドライバにより通信されるデータを制御するセキュリティモジュールと、を有する装置。

【請求項77】 セキュリティ構成データ要素に接続され、その状態を制御するセキュリティ構成制御モジュールを有する請求項76に記載の装置。

【請求項78】 セキュリティ構成制御モジュールに接続されたディスク構成データ要素を有し、セキュリティ構成制御モジュールは、ディスク構成データ要素の状態にしたがって、セキュリティ構成データ要素の状態を制

御する請求項77に記載の装置。

【請求項79】 ディスク構成データ要素に接続され、その状態を制御する外部インタフェースモジュールを有し、外部インタフェースモジュールは記憶装置に提供されたコマンドデータを受け取る請求項78に記載の装置。

【請求項80】 外部モジュールはオーバーライド表示データ要素に接続されてその状態を制御する請求項79に記載の装置。

【請求項81】 オーバーライド表示データ要素に接続され、経過時間量にしたがってその状態を制御するカウンタモジュールを有する請求項80に記載の装置。

【請求項82】 記憶装置のポートで受信したシステムコマンドを実行するか否かを決定する方法において、オープンオーバーライドが設定されているか否かを決定するステップと、

ポート制御データが存在するか否かを決定するステップと

ポート制御データが、システムコールが許容されることを示しているか否かを決定するステップと、

システムコールが許容されることを示すポート制御データ、設定中のオープンオーバーライド、および存在しないポート制御データの少なくとも1つに応じてシステムコールを実行するステップと、を有する方法。

【請求項83】 クローズオーバーライドが設定されたか否かを決定するステップと、

設定中のクローズオーバーライドおよびシステムコールが許容されないことを示すポート制御データの少なくとも1つに応じてシステムコールを拒絶するステップと、を有する方法。

【請求項84】 データ記憶装置の制御方法において、記憶装置にアクセスする少なくとも1つの要求元を提供するステップと、

データ記憶装置の装置の少なくとも1つのプールを提供するステップと、

複数のアクセスタイプを提供するステップと、装置のプールの少なくとも1つの装置について、少なくとも1つの要求元グループの要求元による要求が許容されたか否かを決定するステップと、を有し、装置は、要求の対象である方法。

【請求項85】 アクセスタイプは、ミラーリング、コピー、バックアップ分割およびトラッキングシステムコールの少なくとも1つを含む請求項84に記載の方法。

【請求項86】 アクセスタイプは、データの読み取りおよび書き込みを含む請求項84に記載の方法。

【請求項87】 少なくとも1つのグループと少なくとも1つのプールは、唯一のIDナンバーと物理的ユニットを有する少なくとも1つの論理的ユニットを含む請求項84に記載の方法。

【請求項88】 少なくとも1つのプールは、データ記

憶装置の通信ポートおよびデータ記憶装置のメモリの部分の少なくとも1つを含む請求項84に記載の方法。

【請求項89】 プールは通信ポートを有し、アクセス権はシステムコールが通信ポート上で許容されたか否かを示す請求項88に記載の方法。

【請求項90】 プールはメモリの部分を含み、アクセス権はセクションへの読み出しおよび書き込みアクセスの少なくとも1つを示す請求項88に記載の方法。

【請求項91】 データ記憶装置へのアクセス制御方法において、

データ記憶装置へのアクセスを有する各要求元について、各要求元を唯一に識別する要求元識別ナンバーを提供するステップと、

データ記憶装置のメモリを複数のメモリセグメントに分割し、各セグメントについて識別ナンバーを規定するステップと、

読み取り、書き込み、ミラーリング、コピー、バックアップ、分割およびトラッキングシステムコールの少なくとも1つを含む複数の要求タイプを提供するステップと、

要求元識別ナンバーにしたがって、選択されたメモリセグメントへの選択されたタイプの要求が許容されたことを要求元識別ナンバーのデータベースが示す場合にのみ、複数のメモリセグメントの選択された1つへの選択されたタイプの要求アクセスを要求元に許容するステップと、を有する方法。

【請求項92】 識別ナンバーが特定のメモリセグメントへの特定タイプのアクセスを許容されないことをデータベースが示す場合に、アクセス要求否定表示を発するステップを有する請求項91に記載の方法。

【請求項93】 オーバーライドメモリ位置が、バスオーバーライド条件、拒絶オーバーライド条件およびオーバーライド無し条件の少なくとも1つを記憶する請求項91に記載の方法。

【請求項94】 データベースの審査前にオーバーライドメモリ位置がチェックされ、バスオーバーライド条件が記憶されている場合に、要求が許容される請求項93に記載の方法。

【請求項95】 オーバーライドメモリ位置に記憶された値は指定時間後にオーバーライド無し条件に復帰する請求項94に記載の方法。

【請求項96】 指定時間は30分である請求項95に記載の方法。

【請求項97】 データベースの審査前にオーバーライドメモリ位置がチェックされ、拒絶オーバーライド条件が記憶されている場合に、要求が否定される請求項93に記載の方法。

【請求項98】 複数のメモリセグメントが装置のプールにグループ化され、要求元に選択されたタイプの要求アクセスを許容することは、選択されたメモリセグメン

トに対応する装置のプールの特定の1つを審査することを含む請求項91に記載の方法。

【請求項99】 データ記憶装置へのアクセス制御方法において、データ記憶装置の特定部分のデータの読み取り、データ記憶装置の特定部分へのデータの書き込み、データ記憶装置の特定部分からのデータのバックアップ、データのミラーリング、データ記憶装置の特定部分からのデータのコピー、データ記憶装置のボリュームの分割、およびデータ記憶装置のボリュームへのトラッキング変更の少なくとも1つの要求を発行することにより、データ記憶装置にアクセスする複数の要求元装置から少なくとも1つのグループの要求元装置を提供するステップと、

データ記憶装置の複数の個別アドレス可能メモリリソースから複数のメモリリソースのプールを提供するステップと、

メモリにアクセスする前に、データ記憶装置の制御ロジックを提供して、複数のプールのメモリリソースの少なくとも1つへアクセスするための複数の要求元装置の1つからの要求が許容可能か否かを決定するステップと、を有する方法。

【請求項100】 オーバーライドメモリ位置は、バスオーバーライド条件、拒絶オーバーライド条件、およびオーバーライド無し条件のうちの1つを記憶する請求項99に記載の方法。

【請求項101】 データベースの審査前にオーバーライドメモリ位置がチェックされ、バスオーバーライド条件が記憶されている場合に要求が許容される請求項100に記載の方法。

【請求項102】 オーバーライドメモリ位置に記憶された値は、特定時間後にオーバーライド無し条件に復帰する請求項101に記載の方法。

【請求項103】 特定時間は30分である請求項102に記載の方法。

【請求項104】 データベースの審査前にオーバーライドメモリ位置がチェックされ、拒絶オーバーライド条件が記憶されている場合に、要求が否定される請求項100に記載の方法。

【請求項105】 要求元に対応するグループについてのアクセスレベルは、要求元のグループのあらゆるメンバーについて設定されたアクセスレベルより低いアクセスレベルを提供するように設定される請求項99に記載の方法。

【請求項106】 要求元のアクセスレベルの前にグループのアクセスレベルが審査され、グループへのアクセスが許容された場合は要求元のアクセスレベルについてのチェックは行われず請求項105に記載の方法。

【請求項107】 メモリリソースのプールは、プールのあらゆるメンバーについて設定されたアクセスレベルより多いアクセスレベルを許容する請求項99に記載の

方法。

【請求項108】 メモリセグメントのアクセスレベルより前にブールのアクセスレベルが審査され、ブールへのアクセスが許容されない場合、メモリセグメントのアクセスレベルのチェックは行われない請求項107に記載の方法。

【請求項109】 データ記憶装置へのアクセス制御方法において、

記憶要素へのアクセスを有する要求元および要求元が属するグループの少なくとも1つを識別するIDナンバーを関連付けるステップと、

アクセス情報にしたがって、データ記憶装置の少なくとも1部分への要求されたタイプのアクセス動作が要求元に許容されたか否かを決定するステップと、を有し、アクセス情報は、要求元IDナンバー、グループのIDナンバー、要求元に対応するパスワードおよびグループに対応するパスワードの少なくとも1つに関連する1つ以上のアクセス動作を含む方法。

【請求項110】 アクセス動作は、バックアップ、ミラー、コピー、分割およびトラックの少なくとも1つを含む請求項109に記載の方法。

【請求項111】 アクセス動作は、データ読み取りおよびデータ書き込みの少なくとも1つを含む請求項110に記載の方法。

【請求項112】 アクセス情報は、要求元IDナンバー、グループのIDナンバー、要求元に対応するパスワード、およびグループに対応するパスワードの1つのみを使用する請求項110に記載の方法。

【請求項113】 アクセス情報は、要求元IDナンバーとグループのIDナンバーの組み合わせを使用する請求項110に記載の方法。

【請求項114】 アクセス情報は、グループのIDナンバーと、要求元に対応するパスワードおよびグループに対応するパスワードの少なくとも1つとの組み合わせを使用する請求項110に記載の方法。

【請求項115】 アクセス情報は、グループのIDナンバーとグループに対応するパスワードとの組み合わせを使用する請求項110に記載の方法。

【請求項116】 データ記憶装置へのアクセス制御方法において、

記憶要素へのアクセスを有する要求元および要求元が属するグループへの少なくとも1つを識別するパスワードを関連付けするステップと、

アクセス情報にしたがって、データ記憶装置の少なくとも1部分への要求されたタイプのアクセス動作が要求元に許容されたか否かを決定するステップと、を有し、アクセス情報はパスワードに関連する1つ以上のアクセス動作を含む方法。

【請求項117】 アクセス動作は、バックアップ、ミラー、コピー、分割およびトラックの少なくとも1つを

含む請求項116に記載の方法。

【請求項118】 アクセス動作は、データ読み取りおよびデータ書き込みの少なくとも1つを含む請求項116に記載の方法。

【請求項119】 パスワードは要求元に対応する請求項116に記載の方法。

【請求項120】 パスワードはグループに対応する請求項116に記載の方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、コンピュータデータ記憶装置の分野に関し、特にデータ記憶装置への制御システムコールアクセスを構成する分野に関する。

【0002】

【従来の技術】ホストシステムは、複数のホストインタフェースユニット（ポート）を含むデータ記憶装置を使用してデータを記憶および検索することができ、そのホストインタフェースユニットはデータ記憶装置内に設けられた内部記憶機構と通信し、データを記憶および検索することができる。そのようなデータ記憶装置は、例えばマサチューセッツ州ホプキントンのEMCコーポレーションにより提供され、Yanai et al.の米国特許第5,206,939号、Galtzur et al.の米国特許第5,778,394号、Vishnitzky et al.の米国特許第5,845,147号およびOfekの米国特許第5,857,208号に記載されている。

【0003】ホストシステムには、内部記憶機構の特定部分への制限されたアクセスが与えられることがあり、そのアクセスはデータの読み書き、およびデータ記憶装置に管理類似の動作（例えば、自動ミラーリング、コピー、バックアップ）を実行させる「システムコール」を含むことができる。システムコールは直接的にデータを読み書きするものではない。しかし、そうであっても、システムコールは、ユーザホストシステムの1つを別の1つのホストシステムに割り当てられたデータに間接的にアクセスさせることができる。加えて、遠くの記憶装置（例えば災害復旧状況において）またはファブリック（fabric）ポートを通じて記憶素子リモートシステムコールを発行することができる。

【0004】

【発明が解決しようとする課題】1つのホストシステムに対して別の1つのホストシステムに割り当てられたメモリリソースへの意図的でない間接的アクセスを提供するシステムコールの使用は、全てのホストシステムと記憶装置全体が、単一のエンティティであってそのエンティティ内の異なるグループ間のアクセスを調整可能なエンティティ（すなわち、全てが単一の企業により所有され動作される）により制御される場合は、問題とはならない。しかし、全てのホストシステムが単一のエンティティによって制御されるわけではない場合（例えば、複数の異なる小企業が1つのデータ記憶装置を共用する場

合)、および同一企業の異なるグループが無調整な方法でホストシステムにアクセスする場合、システムコールを使用して内部記憶機能のそのような間接的アクセスを許容することは、特にデータ記憶装置が1つ以上のエンティティおよび/または単一エンティティ内の1つ以上のグループの機密データを含む場合には、望ましくない。さらに、記憶装置が追加の記憶装置に接続されてそのためのバックアップサービスを提供する構成においては、システムコールによりデータへの意図しないアクセスを許容することは望ましくない。

【0005】

【課題を解決するための手段】本発明によれば、記憶装置の制御は、記憶装置にアクセスする少なくとも1つグループを規定すること、記憶装置の装置の少なくとも1つのプールを規定すること、複数のアクセスタイプを規定すること、少なくとも1つのグループについて、アクセスタイプの少なくとも1つについて少なくとも1つのプールに関するアクセス権を決定すること、を含む。アクセスタイプは、システムコールを含むことができる。少なくとも1つのグループおよび少なくとも1つのプールは、論理的または物理的ユニットを含むことができる。少なくとも1つのプールは、記憶装置の通信ポートを含むことができる。アクセス権は、通信ポート上でシステムコールが許容されるか否かを示すことができる。

【0006】さらに本発明によれば、記憶装置へのアクセス制限は、記憶装置に設けられた複数のポートのうちの1つにより複数のホストシステムの各々を記憶装置へ接続すること、各ポートについて、システムコールが許容されるか否かを選択的に決定すること、を含み、システムコールが許容されないポートについては、そのポートに接続されたホストシステムによるシステムコールが記憶装置に、システムコールが実行されなかったことを示させる。また、アクセスの制限は、ポートがシステムコールを許容できるか否かを制御するメカニズムを提供することを含む。メカニズムを提供することは、記憶装置に接続された外部制御装置を提供することを含む。外部制御装置は、記憶装置へキャラクタを送信するとともに記憶装置からキャラクタを受信するダムターミナルとして機能することができる。

【0007】また、アクセスの制限は、システムコールを許容しないポート上のシステムコールを許容するオーバーライドメカニズムを提供することを含む。また、オーバーライドメカニズムは、システムコールを許容するポート上のシステムコールを阻止することができる。また、アクセスの制限は、メカニズムが設定されてから所定時間量の経過後にオーバーライドメカニズムをリセットすることを含む。所定時間量は、30分とすることができる。また、アクセスの制限は、オーバーライドメカニズムの設定を容易化する外部制御装置を提供すること

を含む。外部制御装置を提供することは、記憶装置へキャラクタを送信するとともに記憶装置からキャラクタを受信するダムターミナルを提供することを含む。

【0008】さらに本発明によれば、記憶装置のポートは、記憶装置へ提供されたデータを受信する手段と、記憶装置からデータを送信する手段と、ポートへ提供されたシステムコールを禁止する手段と、を有し、システムコールは、データを送受信しない記憶装置についての管理動作の要求を含む。

【0009】さらに本発明によれば、記憶装置上のポートを制御するコンピュータソフトウェアは、記憶装置と通信する手段と、通信する手段に接続され、提供されたシステムコマンドをポートが受け取らないようにする記憶装置へのコマンドを提供する制御手段と、を有し、システムコマンドは記憶装置による管理動作の要求を含む。

【0010】さらに本発明によれば、記憶装置上のポートを制御する装置は、ポートに接続され、記憶装置とのデータ通信を処理するポートドライバと、ポートドライバに接続され、セキュリティ構成データ要素とオーバーライド表示データ要素に基づいてポートドライバにより通信されたデータを制御するセキュリティモジュールと、を含む。また、その装置は、セキュリティ構成データ要素に接続され、その状態を制御するセキュリティ構成制御モジュールを含むことができる。また、その装置は、セキュリティ構成制御モジュールに接続されたディスク構成データ要素を含むことができ、セキュリティ構成制御モジュールはディスク構成データ要素の状態にしたがってセキュリティ構成データ要素の状態を制御する。また、その装置は、ディスク構成データ要素に接続され、その状態を制御する外部インタフェースモジュールを含み、外部インタフェースモジュールは記憶装置へ提供されるコマンドデータを受信する。外部モジュールは、オーバーライド表示データ要素に接続され、その状態を制御することができる。また、その装置はオーバーライド表示データ要素に接続され、経過時間量にしたがってその状態を制御するカウンタモジュールを含むことができる。

【0011】さらに本発明によれば、記憶装置のポートで受信したシステムコマンドを実行するか否かを決定することは、オープンオーバーライドが設定されているか否かを決定すること、ポート制御データが存在するか否かを決定すること、ポート制御データは、システムコールが許容されることを示しているか否かを決定すること、システムコールが許容されることを示すポート制御データ、設定中のオープンオーバーライド、および存在しないポート制御データの少なくとも1つに応じてシステムコールを実行すること、を含む。また、システムコマンドを実行するか否かを決定することは、クローズオーバーライドが設定されたか否かを決定すること

と、設定中のクローズオーバーライドおよびシステムコールが許容されないことを示すポート制御データの少なくとも1つに応じてシステムコールを拒絶すること、を含むことができる。

【0012】さらに本発明によれば、データ記憶装置の制御方法は、記憶装置にアクセスする少なくとも1つの要求元を提供すること、データ記憶装置の装置の少なくとも1つのプールを提供すること、複数のアクセスタイプを提供すること、装置のプールの少なくとも1つの装置について、少なくとも1つの要求元グループの要求元による要求が許容されたか否かを決定すること、を含み、装置は、要求の対象である。アクセスタイプは、ミラーリング、コピー、バックアップ、分割およびトラッキングシステムコールの少なくとも1つを含むことができる。アクセスタイプは、さらにデータの読み取りおよび書き込みを含むことができる。少なくとも1つのグループと少なくとも1つのプールは、唯一のIDナンバーと物理的ユニットを含む少なくとも1つの論理的ユニットを含むことができる。少なくとも1つのプールは、データ記憶装置の通信ポートおよびデータ記憶装置のメモリの部分の少なくとも1つを含むことができる。プールは通信ポートを含むことができ、アクセス権はシステムコールが通信ポート上で許容されたか否かを示す。プールはメモリの部分を含むことができ、アクセス権はセクションへの読み出しおよび書き込みアクセスの少なくとも1つを示す。

【0013】さらに本発明によれば、データ記憶装置へのアクセス制御方法は、データ記憶装置へのアクセスを有する各要求元について、各要求元を唯一に識別する要求元識別ナンバーを提供すること、データ記憶装置のメモ리를複数のメモリセグメントに分割し、各セグメントについて識別ナンバーを規定すること、読み取り、書き込み、ミラーリング、コピー、バックアップ、分割およびトラッキングシステムコールの少なくとも1つを含む複数の要求タイプを提供すること、要求元識別ナンバーにしたがって、選択されたメモリセグメントへの選択されたタイプの要求が許容されたことを要求元識別ナンバーのデータベースが示す場合にのみ、複数のメモリセグメントの選択された1つへの選択されたタイプの要求アクセスを要求元に許容すること、を含む。アクセス制御方法は、識別ナンバーが特定のメモリセグメントへの特定タイプのアクセスを許容されないことをデータベースが示す場合に、アクセス要求否定表示を発することを含むことができる。オーバーライドメモリ位置は、バスオーバーライド条件、拒絶オーバーライド条件およびオーバーライド無し条件の少なくとも1つを記憶することができる。データベースの審査前にオーバーライドメモリ位置をチェックし、バスオーバーライド条件が記憶されている場合に、要求を許容することができる。オーバーライドメモリ位置に記憶された値は指定時

間後にオーバーライド無しに復帰することができる。指定時間は30分とすることができる。データベースの審査前にオーバーライドメモリ位置をチェックし、拒絶オーバーライド条件が記憶されている場合に、要求を否定することができる。複数のメモリセグメントを装置のプールにグループ化することができ、要求元に選択されたタイプの要求アクセスを許容することは、選択されたメモリセグメントに対応する装置のプールの特定の1つを審査することを含むことができる。

【0014】さらに本発明によれば、データ記憶装置へのアクセス制御方法は、データ記憶装置の特定部分のデータの読み取り、データ記憶装置の特定部分へのデータの書き込み、データ記憶装置の特定部分からのデータのバックアップ、データのミラーリング、データ記憶装置の特定部分からのデータのコピー、データ記憶装置のボリュームの分割、およびデータ記憶装置のボリュームへのトラッキング変更の少なくとも1つの要求を発行することにより、データ記憶装置にアクセスする複数の要求元装置から少なくとも1つのグループの要求元装置を提供すること、データ記憶装置の複数の個別アドレス可能メモリリソースから複数のメモリリソースのプールを提供すること、メモリにアクセスする前に、データ記憶装置の制御ロジックを提供して、複数のプールのメモリリソースの少なくとも1つへアクセスするための複数の要求元装置の1つからの要求が許容可能か否かを決定すること、を含む。オーバーライドメモリ位置は、バスオーバーライド条件、拒絶オーバーライド条件、およびオーバーライド無し条件のうちの1つを記憶することができる。データベースの審査前にオーバーライドメモリ位置をチェックすることができ、バスオーバーライド条件が記憶されている場合に要求を許容することができる。オーバーライドメモリ位置に記憶された値は、特定時間後にオーバーライド無し条件に復帰することができる。特定時間は30分とすることができる。データベースの審査前にオーバーライドメモリ位置をチェックすることができ、拒絶オーバーライド条件が記憶されている場合に、要求を否定することができる。要求元に対応するグループについてのアクセスレベルは、要求元のグループのあらゆるメンバーについて設定されたアクセスレベルより低いアクセスレベルを提供するように設定することができる。要求元のアクセスレベルの前にグループのアクセスレベルを審査することができ、グループへのアクセスが許容された場合は要求元のアクセスレベルについてのチェックは行われない。メモリリソースのプールは、プールのあらゆるメンバーについて設定されたアクセスレベルより多いアクセスレベルを許容することができる。メモリセグメントのアクセスレベルより前にプールのアクセスレベルを審査することができ、プールへのアクセスが許容されない場合、メモリセグメントのアクセスレベルのチェックは行われない。

【0015】さらに本発明によれば、データ記憶装置へのアクセス制御方法は、記憶要素へのアクセスを有する要求元および要求元が属するグループの少なくとも1つを識別するIDナンバーを関連付けることと、アクセス情報にしたがって、データ記憶装置の少なくとも1部分への要求されたタイプのアクセス動作が要求元に許容されたか否かを決定することと、を含み、アクセス情報は、要求元IDナンバー、グループのIDナンバー、要求元に対応するパスワードおよびグループに対応するパスワードの少なくとも1つに関連する1つ以上のアクセス動作を含む。アクセス動作は、バックアップ、ミラー、コピー、分割およびトラックの少なくとも1つを含むことができる。アクセス動作は、データ読み取りおよびデータ書き込みの少なくとも1つを含むことができる。アクセス情報は、要求元IDナンバー、グループのIDナンバー、要求元に対応するパスワード、およびグループに対応するパスワードの1つのみを使用することができる。アクセス情報は、要求元IDナンバーとグループのIDナンバーの組み合わせを使用することができる。アクセス情報は、グループのIDナンバーと、要求元に対応するパスワードおよびグループに対応するパスワードの少なくとも1つとの組み合わせを使用することができる。アクセス情報は、グループのIDナンバーとグループに対応するパスワードとの組み合わせを使用することができる。

【0016】さらに本発明によれば、データ記憶装置へのアクセス制御方法は、記憶要素へのアクセスを有する要求元および要求元が属するグループへの少なくとも1つを識別するパスワードを関連付けすることと、アクセス情報にしたがって、データ記憶装置の少なくとも1部分への要求されたタイプのアクセス動作が要求元に許容されたか否かを決定することと、を含み、アクセス情報はパスワードに関連する1つ以上のアクセス動作を含む。アクセス動作は、バックアップ、ミラー、コピー、分割およびトラックの少なくとも1つを含むことができる。アクセス動作は、データ読み取りおよびデータ書き込みの少なくとも1つを含むことができる。パスワードは要求元またはグループに対応することができる。

【0017】そのような構成によれば、データ記憶装置リソース、特に共用リソースへのコンピュータシステムのアクセスは、集中されているか分散されているかわからず、認可されていない制御、アクセスまたは記憶リソース再構成変化が選択されたメモリ記憶装置のプールに起きることを防止するように制御することができる。そのようなアクセス許可の詳細な制御により、高感度データへ誰がアクセス可能かについての制御を失うことなく、およびメモリ構成の制御を失うことなく、別個の区別されたユーザグループ間で効率的な方法でメモリ記憶リソースを共用することを可能とする。いくつかのシステムでは、システム管理の制限されたセットのみ

が、ホストコンピュータシステムまたは他のユーザのグループからの制御されたアクセスを有するリソースプール内へ利用可能なデータ記憶装置の部分を構成するためのアクセス許可を有することができる。システム管理は、個別メモリリソース要素を種々のメモリ装置プールにグループ化することができ、各プールは要求しているホストシステムの各個別の1つへまたはホストシステムのグループへ異なるレベルのシステムコールアクセスを有する。こうして、記載された構成は、異なるホスト環境および望ましいメモリ構成の要求を満足しつつ、ホストシステムおよびユーザの大グループによるメモリリソースのグループへのアクセスを制御するための単純であるが柔軟性を有する方法を提供する。

【0018】メモリシステムアクセスを要求しているホストシステム（すなわち、要求元）は、個別の大型コンピュータシステムとすることができ、各個別のものは複数のリアルタイムまたはバッチユーザ、ローカルエリアネットワークを通じてメインメモリに接続されたパーソナルコンピュータのワークグループ、または、ルーチンバックアップ記憶機能を実行する他のデータ記憶装置、もしくはデータ記憶装置に接続可能な他の多数の既知の電子装置を有する。データ記憶装置は、個別磁気メモリディスクの大型アレイ、大型マストレージディスクのアドレス可能部分、半導体メモリ、メモリシステムの通信アクセスポート、またはあらゆる多数の既知の形態のデータ記憶装置を使用してセットアップすることができる。

【0019】記載された実施形態は、メモリへのアクセスを要求できる各ホストシステムのID、各利用可能なメモリ要素のID、および、各メモリ要素において各ホストIDがどのタイプのアクセスを許容されるか、を含むマトリクスに基づいてメモリの部分を選択する制限されたアクセスを可能とする。要求元IDは、既存のホストコンピュータシステムハードウェアID、マルチコンピュータシステム内のユーザパスワードまたはグループパスワード、ファイバチャンネルワールドワイドネーム、インターネットアクセス構成におけるURL、メモリシステムにより割り当てられたユニークランダムアクセスナンバー、デフォルト値、もしくは要求によりアドレスされたメモリセグメントへの許容可能なアクセス件をチェックする目的で要求装置を識別するための機能できるあらゆるナンバーを使用して作り出すことができる。そのようなチェックは、典型的にはマトリクスの形態のアドレスされたメモリの許容可能な要求元のデータベースに対してIDを比較することにより実行される。例えば、111AAA2というハードウェアIDを有する大型ホストコンピュータシステムは10個の端末と50個の認可ユーザアカウントを有することができる。50のユーザ全てが集中メモリの各部分へのアクセスをホストシステムアドミニストレータにより許可されたなら

ば、記憶システムをホストコンピュータシステムへ接続する特定のメモリアクセスポートのIDナンバーにしたがって単純にアクセスを許容することにより適切なアクセスを得ることができる。しかし、50のユーザが5つの異なるワークグループに属し、その各グループがそのデータ記憶領域を他の4つのワークグループのアクションにより影響を受けたくないと考えるならば、アクセスは、50全てのユーザに共通の共用メモリセクションへのアクセスを与えるハードウェアIDと、大型ホストコンピュータに割り当てられたメモリ領域所定部分への増加するアクセスを提供する個別ユーザパスワードとの組み合わせによって許容することができる。別の例は、インターネットを通じてアクセス可能な大型メモリシステムである。インターネット接続された多数のコンピュータ各々によりアドレス可能な特定のメモリリソースは、あらゆるタイプのノーアクセスから、要求元のURLにより許容されたメモリセクションのIDナンバーまたはその代わりに割り当てアクセスIDナンバーに依存して、アドレスされたメモリセクションへのシステムコールアクセスを完了する。

【0020】記載された方法は、読み取りのみのノーアクセスから、コピーまたはミラーなどのシステムコール、もしくはアクセス制御ロジック中に規定され含まれるあらゆるレベルのシステムアドミニストレータアクセスなどにわたるアドレスされたメモリ要素またはセクションへのあらゆるレベルの要求元アクセスを可能とする。複数の要求元は同一のメモリ要素への異なるレベルのアクセスを有することができ、要求元は、唯一のグループIDナンバーと特定のメモリ要素への規定されたアクセスを有する複数の便利な要求元グループへグループ化することができる。グループと要求元の両方にIDが割り当てられる実施形態では、グループIDはグループのあらゆる個別メンバーがデバイスプールに関して有する最低アクセスレベル以下のデバイスプールへのアクセスレベルに対応する。そのような構成は、認可された要求元より迅速にアクセスが許可されることを可能とする。なぜなら、グループIDを見つけ許可可能なアクセス制限を決定するためにサーチすべきアクセス制御ロジックメモリは、各個別要求元についての場合よりも小さいであろう。

【0021】同様に、複数のメモリ要素を、メモリ装置および所定のプールIDナンバーにグループ化することができる。メモリ要素は、別個の磁気ディスク、ディスクの部分、接続されたディスクのグループ、キャッシュなどの半導体メモリ、またはデータ記憶装置を要求元またはホストコンピュータシステムへ接続する通信ポートとすることができる。いくつかのシステムでは、プールは要求元IDに関してあらゆる1人のプールメンバーより多くのアクセスを許容し、よって要求元がプールをアドレスするのに十分なアクセスを有しないと分かった場

合、さらなるサーチは行われず、効率およびアクセス速度が改善される。

【0022】さらに本発明によれば、アクションの許可を決定することは、複数のグループを規定することと、各グループについて、複数のアクションタイプと、対応する許可レベルとを規定することと、少なくともアクションタイプのサブセットについて、対応するアクションを実行する複数の装置を規定することであって、少なくともいくつかの装置はデータ記憶装置の部分に対応することと、少なくとも1つのグループについて、要求されたアクションについての許可を決定することと、を含み、アクションが装置の1つに対応する場合に、少なくとも1つのグループに対応するアクションタイプについて許可レベルを調べることで、および要求されたアクションに対応する複数の装置を調べることで許可が決定され、アクションが装置の1つに対応しない場合に、少なくとも1つのグループに対応するアクションタイプについての許可レベルを調べることで許可が決定される。アクションタイプはデータ記憶装置へのシステムコールを含むことができる。少なくとも1つの装置は、データ記憶装置の少なくとも1つのディスク記憶領域を含むことができる。少なくとも1つの装置は、データ記憶装置の通信ポートを含むことができる。アクションタイプは、システムコールが通信ポート上で許容されるか否かを示すことができる。許可されている要求されたアクションに対して、アクションを実行する後続の要求に関して使用可能なタグを返すことができる。

【0023】さらに本発明によれば、アクションに対する許可を決定することにおいて、要求者が要求者リストに含まれるか否かを決定することと、要求されたアクションが要求者に関連するアクションタイプのリスト中に含まれるか否かを決定することと、アクションが少なくとも1つの装置を使用する場合に、少なくとも1つの装置が要求者及び要求されたアクションに関連する装置リスト中に含まれるか否かを決定することと、を含み、装置リストはデータ記憶装置に関連する少なくともいくつかの装置を含む。また、許可を決定することは、要求者が要求者リスト中に含まれない場合、要求者リストからデフォルト要求者を使用することを含むことができる。また、許可を決定することは、要求者が要求者リストに含まれない場合に、許可を否定することを含むことができる。また、許可を決定することは、要求されたアクションが少なくとも1つの装置を使用しない場合、要求されたアクションが要求者に関連付けされたアクションタイプのリストに含まれる場合にアクションを許可することを含むことができる。アクションタイプの少なくともいくつかはデータ記憶装置上で実行されるアクションに対応しないものとできる。アクションタイプはデータ記憶装置へのシステムコールを含むことができる。少なくとも1つの装置は、データ記憶装置の少なくとも1つの

ディスク記憶領域を含むことができる。少なくとも1つの装置は、データ記憶装置の通信ポートを含むことができる。アクションタイプは、通信ポート上でシステムコールが許可されるか否かを示すことができる。また、許可を決定することは、許可されている要求されたアクションに対して、アクションを実行する後続の要求に関連して使用可能なタグを返すことを含むことができる。

【0024】さらに本発明によれば、アクションの許可を決定する装置は、複数のグループを規定する手段と、各グループについて、複数のアクションタイプと、対応する許可レベルとを規定する手段と、少なくともアクションタイプのサブセットについて、対応するアクションを実行する複数の装置を規定する手段であって、少なくともいくつかの装置はデータ記憶装置の部分に対応する手段と、少なくとも1つのグループについて、要求されたアクションについての許可を決定する手段と、を有し、アクションが装置の1つに対応する場合に、少なくとも1つのグループに対応するアクションタイプについて許可レベルを調べることで、および要求されたアクションに対応する複数の装置を調べることにより許可が決定され、アクションが装置の1つに対応しない場合に、前記少なくとも1つのグループに対応するアクションタイプについての許可レベルを調べることにより許可が決定される。アクションタイプはデータ記憶装置へのシステムコールを含むことができる。少なくとも1つの装置は、データ記憶装置の少なくとも1つのディスク記憶領域を含むことができる。少なくとも1つの装置は、データ記憶装置の通信ポートを含むことができる。アクションタイプは、システムコールが通信ポート上で許可されるか否かを示すことができる。許可されている要求されたアクションに対して、装置はアクションを実行する後続の要求に関して使用可能なタグを返すことができる。

【0025】さらに本発明によれば、アクションに対する許可を決定する装置は、要求者が要求者リストに含まれるか否かを決定する手段と、要求されたアクションが要求者に関連するアクションタイプのリスト中に含まれるか否かを決定する手段と、アクションが少なくとも1つの装置を使用する場合に、少なくとも1つの装置が要求者及び要求されたアクションに関連する装置リスト中に含まれるか否かを決定する手段と、を有し、装置リストはデータ記憶装置に関連する少なくともいくつかの装置を含む。また、その装置は、要求者が要求者リスト中に含まれない場合、要求者リストからデフォルト要求者を使用する手段を有することができる。また、その装置は、要求者が要求者リストに含まれない場合に、許可を否定する手段を有することができる。また、その装置は、要求されたアクションが少なくとも1つの装置を使用しない場合、要求されたアクションが要求者に関連付けられたアクションタイプのリストに含まれる場合にアクションを許可する手段を有することができる。アクション

タイプは、少なくともいくつかはデータ記憶装置上で実行されるアクションに対応しないものとして行うことができる。アクションタイプはデータ記憶装置へのシステムコールを含むことができる。少なくとも1つの装置は、データ記憶装置の少なくとも1つのディスク記憶領域を含むことができる。少なくとも1つの装置は、データ記憶装置の通信ポートを含むことができる。アクションタイプは、通信ポート上でシステムコールが許可されるか否かを示すことができる。また、その装置は、許可されている要求されたアクションに対して、アクションを実行する後続の要求に関連して使用可能なタグを返す手段を有することができる。

【0026】さらに本発明によれば、アクションの許可を決定するコンピュータソフトウェアにおいて、複数のグループを規定する実行可能なコードと、各グループについて、複数のアクションタイプと、対応する許可レベルとを規定する実行可能なコードと、少なくともアクションタイプのサブセットについて、対応するアクションを実行する複数の装置を規定する実行可能なコードであって、少なくともいくつかの装置はデータ記憶装置の部分に対応する実行可能なコードと、少なくとも1つのグループについて、要求されたアクションについての許可を決定する実行可能なコードと、を有し、アクションが装置の1つに対応する場合に、少なくとも1つのグループに対応するアクションタイプについて許可レベルを調べることで、および要求されたアクションに対応する複数の装置を調べることにより許可が決定され、アクションが装置の1つに対応しない場合に、少なくとも1つのグループに対応するアクションタイプについての許可レベルを調べることにより許可が決定される。アクションタイプはデータ記憶装置へのシステムコールを含むことができる。少なくとも1つの装置は、データ記憶装置の少なくとも1つのディスク記憶領域を含むことができる。少なくとも1つの装置は、データ記憶装置の通信ポートを含むことができる。アクションタイプは、システムコールが通信ポート上で許可されるか否かを示すことができる。許可されている要求されたアクションに対して、アクションを実行する後続の要求に関して使用可能なタグを返す実行可能なコードを有することができる。

【0027】さらに本発明によれば、アクションに対する許可を決定するコンピュータソフトウェアにおいて、要求者が要求者リストに含まれるか否かを決定する実行可能なコードと、要求されたアクションが要求者に関連するアクションタイプのリスト中に含まれるか否かを決定する実行可能なコードと、アクションが少なくとも1つの装置を使用する場合に、少なくとも1つの装置が要求者及び要求されたアクションに関連する装置リスト中に含まれるか否かを決定する実行可能なコードと、を有し、装置リストはデータ記憶装置に関連する少なくともいくつかの装置を含む。そのコンピュータソフトウェア

は、要求者が要求者リスト中に含まれない場合、要求者リストからデフォルト要求者を使用する実行可能なコードを有することができる。そのコンピュータソフトウェアは、要求者が要求者リストに含まれない場合に、許可を否定する実行可能なコードを有することができる。そのコンピュータソフトウェアは、さらに要求されたアクションが少なくとも1つの装置を使用しない場合、要求されたアクションが要求者に関連付けされたアクションタイプのリストに含まれる場合にアクションを許可する実行可能なコードを有することができる。アクションタイプの少なくともいくつかはデータ記憶装置上で実行されるアクションに対応しないものとして行うことができる。アクションタイプはデータ記憶装置へのシステムコールを含むことができる。少なくとも1つの装置は、データ記憶装置の少なくとも1つのディスク記憶領域を含むことができる。少なくとも1つの装置は、データ記憶装置の通信ポートを含むことができる。アクションタイプは、通信ポート上でシステムコールが許可されるか否かを示すことができる。そのコンピュータソフトウェアは、許可されている要求されたアクションに対して、アクションを実行する後続の要求に関連して使用可能なタグを返す実行可能なコードを有することができる。

【0028】

【発明の実施の形態】図1を参照すると、システム20は、データ接続を通じて接続された（図示せず）複数のホストシステムのためのデータを記憶可能なデータ記憶装置22を含む。ホストシステムは、1つ以上のホストプロセッサまたは他のデータ記憶装置を含むことができる。データ記憶装置22は、マサチューセッツ州ホプキントンのEMCコーポレーションが製造するシンメトリックス（Symmetrix）記憶装置、またはここに記述する機能を提供可能な他のタイプのデータ記憶装置を使用して実施することができる。

【0029】データ記憶装置22は、複数のセクション24～26に分割されて図示されており、各セクションは、そこに接続されたホストシステムの1つ（例えば、ホストプロセッサまたは別のデータ記憶装置）によりアクセスされるデータ記憶装置22のリソースの一部を示す。これらのリソースは例えばデータ記憶装置22の内部メモリの部分を含む。

【0030】外部制御装置28は、従来の手法でデータ記憶装置22に接続されてその動作を制御することができる。外部制御装置28はシンメトリックス・シム・ウィン（Symmetrix Symm Win）機能を使用して実施することができ、その機能はマサチューセッツ州ホプキントンのEMCコーポレーションにより提供され、従来のコンピュータワークステーション、ならびにワークステーションとデータ記憶装置22との間の接続および通信を容易化するための他の適切なソフトウェアおよびハードウェア上での動作のためのソフトウェアである。いくつか

の実施形態では、外部制御装置28は、その目的のために提供された従来のソフトウェアを使用してデータ記憶装置22と通信するダムターミナルのように動作する。外部制御装置28が実行する動作は後に詳細に説明される。

【0031】また、データ記憶装置22は複数の外部ポート34～36を有し、それらは記憶装置22に接続されたホストシステムへの通信を提供する。ポート34～36は、ホストシステムがデータ記憶装置22へデータを記憶し、データ記憶装置22からデータを検索することを可能とする。各ポート34～36は、データ記憶装置22に接続されたホストシステムの1つについての通信を処理する。

【0032】データ記憶装置22へ接続されたホストシステムは、データ記憶装置22を制御することができ、ポート34～36を通じて提供可能な管理類似のシステムコールを使用することによりデータ記憶装置22のセクション24～26のアクセスおよび使用を制御することができる。実際、そのようなシステムコールはデータ記憶装置22の構成および動作を制御することができる。いくつかの実施形態では、上述のようにいくつかのシステムコールがデータ記憶装置22内に記憶されたデータに間接的に影響することがあるけれども、システムコールは、単純にポート34～36にデータを読み書きするコールとは区別される。

【0033】データ記憶装置22およびそれに接続された全てのホストシステムが単一のエンティティにより制御される事例では、別のホストシステムの1つによるアクセスに影響を与えることのあるシステムコールをホストシステムに実行させることは簡単である。しかし、ホストシステムが異なるエンティティまたは同一エンティティ内の異なるグループにより制御しうる事例では、異なるエンティティにより制御される別のホストシステムに割り当てられたデータ記憶装置22のセクション24～26のうちの1つに影響を与えるシステムコールを1つのホストシステムが作成することを可能とするのは問題となりうる。言い換えれば、異なるエンティティにより制御されるホストシステムが作成するシステムコールは衝突しうる。

【0034】そのような状況を処理するために、データ記憶装置22のポート34～36のいくつかまたは全てを、それに接続されたホストシステム（または、そのためのあらゆる他の装置）からのシステムコールを受け入れないように構成することができる。システムコールはデータ記憶装置22の構成およびアクセススキームを変形することができるので、ポート34～36のいくつかまたは全てにおいてシステムコールを制限することは、そこに接続されたホストシステムが別のホストシステムに割り当てられたリソースにアクセスすることを禁止する。よって、例えば、セクション24がポート34に接

続されたホストシステムに割り当てられた記憶メモリを示し、セクション 25 がポート 35 に接続されたホストシステムに割り当てられた記憶メモリを示すならば、ポート 34、35 においてシステムコールを禁止することは、例えばポート 34 に接続されたホストシステムがポート 35 に接続されたホストシステムに割り当てられた記憶メモリのセクション 25 に不正にアクセスすることを防止する。後により詳細に説明するように、システムコールにより実行される機能の構成および割り当ては、外部制御装置 28 のみによって、または外部制御装置およびポート 34～36 に接続されたホストシステムのサブセットのみによって実行することができる。

【0035】図 2 を参照すると、システム 40 は、他のデータ記憶装置がもう 1 つの記憶装置に接続されている構成を示す。システム 40 は第 1 のデータ記憶装置 42、第 2 のデータ記憶装置 44、および第 3 のデータ記憶装置 50 を含む。第 1 のデータ記憶装置 42 はポート 52 を通じて第 3 のデータ記憶装置 50 へ接続される。第 2 のデータ記憶装置 44 はポート 54 を通じて第 3 のデータ記憶装置 50 へ接続される。

【0036】図 2 に示すシステム 40 は、例えば第三者データバックアップスキームを示すことができ、そこでは第 1 のエンティティが第 1 のデータ記憶装置 42 を制御し、第 2 の無関係のエンティティが第 2 のデータ記憶装置 44 を制御し、第 1 および第 2 のエンティティ両方が、データ記憶装置 50 を制御する第 3 のエンティティからのデータバックアップサービスを得る。いくつかの例において、データ記憶装置 50 は、第 1 および第 2 のデータ記憶装置 42、44 の位置から離れた位置に設けられる。そのような構成では、ポート 52、54 におけるシステムコールを禁止して、ポート 52 に接続されたデータ記憶装置 42 が、ポート 54 に接続されたデータ記憶装置 44 による使用に割り当てられたデータ記憶装置 50 の部分にアクセスすることを防止することが有益である。同様に、ポート 54 におけるシステムコールを禁止して、データ記憶装置 44 が、データ記憶装置 42 による使用に割り当てられたデータ記憶装置 50 の部分へのアクセスすることを防止することが望ましい。そのようなアクセスを禁止するメカニズムは後により詳細に説明される。

【0037】図 3 を参照すると、データフロー図 60 は、データ記憶装置 22 のポート 34～36 でイーサネットおよびディスエーブルする通信およびシステムコールを処理するソフトウェアの動作を示す。ポートドライバ 62 は、ポート 34 を通じてデータ記憶装置 22 へ提供されたデータを受け取り、データ記憶装置 22 からのデータをポート 34 を通じてそこへ接続されたホストシステム（図示せず）へ供給する。ポート 34 は、ホストシステムとデータ記憶装置 22 との間の通信を提供する。フロー図 60 は、以下の説明を容易にするために、1 つ

のポート 34 と、対応する 1 つのポートドライバのみを示す。しかし、ここに記載された機能は、データ記憶装置 22 のポート 34～36 のいずれかまたは全てに拡張可能であることが当業者に理解されるであろう。

【0038】ポートドライバ 62 はセキュリティモジュール 64 に接続されており、それによりポート 34 を通じてデータ記憶装置 22 に入出力する全てのデータはセキュリティモジュール 64 により制御される。こうして、図 3 に示すように、セキュリティモジュール 64 は、その通常の機能を提供するためにデータ記憶装置 22 の残りの部分との接続を含む。しかし、以下により詳細に説明するように、セキュリティモジュール 64 は特定の状況下においてはデータ記憶装置 22 との間のデータおよび/またはシステムコールの伝送を禁止することができる。セキュリティモジュール 64 の動作は以下により詳細に説明される。

【0039】セキュリティモジュール 64 には、セキュリティ構成データ要素 66 からセキュリティ構成情報が提供される。後により詳細に説明するが、セキュリティ構成データ要素 66 はセキュリティモジュール 64 の動作を制御し、そうしてポートドライバ 62 との間で提供されるデータを制御する。また、セキュリティモジュール 64 には、オーバーライドインジケータデータ要素 67 から情報が提供され、オーバーライドインジケータデータ要素 67 もセキュリティモジュール 64 の動作を制御する。セキュリティ構成制御モジュール 68 はセキュリティ構成データ要素 66 の内容を制御して、ポートドライバ 62 を通じてポート 34 で許容されるアクセスのタイプを示す。セキュリティ構成制御モジュール 68 は、システムコールがポートドライバ 62 により受け入れられたか否か、およびその後データ記憶装置 22 の残りの部分によって処理されたか否かを示すデータを提供することができる。

【0040】いくつかの実施形態では、オーバーライドインジケータデータ要素 67 は、各ポート 34～36 について 1 つの変数を含み、各変数は、オーバーライドなし、オープンオーバーライド、およびクローズオーバーライドのうちの 1 つを示す 3 つの値のうちの 1 つをとる。オープンオーバーライド値は、セキュリティ構成データ要素 66 中の設定にかかわらず、ポート 34～36 のうちの対応する 1 つがシステムコールを受け入れることを示す。同様に、クローズオーバーライド値は、セキュリティ構成データ要素 66 中の設定にかかわらず、ポート 34～36 のうちの対応する 1 つがシステムコールを受け入れないことを示す。

【0041】セキュリティ構成制御モジュール 68 は、データ記憶装置 22 の内部不揮発性領域（例えば、データ記憶装置 22 の全般的制御に使用されるディスクベースの一部に設けられる）に記憶されたディスク構成データ要素 70 からデータを取得する。ディスク構成デー

タ要素70は、データ記憶装置22のポート34～36の各々に許容されるアクセスのタイプに関する情報を含む。

【0042】外部インタフェースモジュール72は、外部制御装置28と通信するための従来からのソフトウェアを含む。外部インタフェースモジュール72は、ディスク構成データ要素70を変形してデータ記憶装置22のポート34～36の各々に提供されるアクセスのタイプを示すためのメカニズムを提供する。後により詳細に説明するように、外部インタフェースモジュール72は、オーバーライドインジケータデータ要素67に書き込むことにより、セキュリティ構成データ要素66のデータをオーバーライドするためのメカニズムを提供することができる。オーバーライドは、永久的なものとしてでき、または例えば30分などの所定時間量に設定することができる。オーバーライドが所定時間量に設定されている場合、カウンタモジュール74がオーバーライドインジケータデータ要素67と相互作用して、その時間後にオーバーライドをリセットする。このためのメカニズムは後に詳しく説明する。

【0043】図4を参照すると、フローチャート80はここに記載されるシステムの動作を示す。第1のテストステップ82において、オープンオーバーライドが設定されたか否かが決定される。オープンオーバーライドは、適当なアクセスセキュリティを有する外部制御装置28のユーザが、ポート34～36の1つ以上のセキュリティについてデフォルト設定のオーバーライドが望まれることを示した時に生じる。そうであれば、それにしたがって、ユーザは外部インタフェースモジュール72を使用してオーバーライド表示データ要素67にアクセスする。1つの実施形態では、オープンオーバーライドはシステム制御セキュリティを有するユーザにより設定することができる。設定されてから所定時間量のみ存在することができる。タイムリミットは、図3のカウントモジュール74によって従来の方で実施することができる。その方法は、オープンオーバーライドが設定された後に所定時間量（例えば30分）をカウントし、所定時間量後に適当にリセットを提供してオーバーライド無しを示す。

【0044】テストステップ82において、オープンオーバーライドが設定されていることが決定されると、次に制御はテストステップ82からステップ84に移行し、そのポートで要求されるシステムコールが実行される（すなわち、システムコールがデータ記憶装置22の残りの部分へ送られる）。ポート34についての他のあらゆる構成設定にかかわらず、オープンオーバーライドが設定されているならば、ポート34に与えられる全てのシステムコールは、オープンオーバーライドが有効状態を維持する限り実行される。

【0045】ステップ82でオープンオーバーライドが

設定されていないことが決定された場合、次に制御はテストステップ82からテストステップ86へ移行し、そこでクローズオーバーライドが設定されているか否かが決定される。オープンオーバーライドの場合と同じように、クローズオーバーライドが設定されていることは、ポート34についてのあらゆる他の設定にかかわらず、クローズオーバーライドが有効状態を維持する限り、そのポートにおいてシステムコールは許容されないことを示す。また、オープンオーバーライドと同様に、クローズオーバーライドは所定時間量、例えば30分設定することができ、その後カウンタモジュール74を使用してリセットされる。

【0046】ステップ86においてクローズオーバーライドが設定されていることが決定されたなら、次に制御はテストステップ86からステップ88へ移行し、そこでポート34に接続されたホストシステムにより要求されたシステムコールが拒絶される。ステップ88でシステムコールを拒絶することは、システムコールにより命じられた動作を実行せず、システムコールが拒絶されたことを示すコードを要求したホストシステムへ返すことを含む。

【0047】テストステップ86の次はテストステップ90であり、それはそのポートについての構成情報が存在するか否かを決定する。いくつかの実施形態において、セキュリティ構成データ要素66を完全に除去する（または、その代わりに、まずセキュリティ構成データ要素66を作成しない）ことができ、その場合にはセキュリティは存在しないと仮定され、よって全てのシステムコールをポート34～36のあらゆるポートで要求することができる。こうして、テストステップ90において構成情報が無い（すなわち、セキュリティ構成データ要素66が無い）と決定された場合、制御はテストステップ90からステップ84へ進み、そこでシステムコールが実行される。

【0048】テストステップ90において構成データがある（すなわち、セキュリティ構成データ要素66がある）と決定された場合、制御はテストステップ90からテストステップ92へ移行し、そこで構成情報を調べ、システムコールがポート34を通じて要求できるか否かが決定される。これは従来の方の方法のうちのいずれか1つによってセキュリティ構成データ要素66中で示すことができ、その従来の方の方法は、各ポートについてシステムコールが各ポートで許容されたか否かを示すブール変数（フラグ）を有することを含む。テストステップ92においてシステムコールが許容されないことが決定された場合、次に制御はステップ92からステップ88へ進み、そこで上述のように要求されたシステムコールが拒絶される。その代わりに、ステップ92においてシステムコールが許容されたことが決定されると、次に制御はテストステップ92からステップ84へ進み、そこ

システムコールが実行される。

【0049】ここに記載される手法を一般化して、情報の要求元のアイデンティティ（すなわち、ホストシステムの識別子）に基づいて動作が実行され、リソースが割り当てられるようにすることができることを述べておく。よって、特定の動作を実行するために要求元の識別子（または要求元のグループ）に特定のアクセスタイプまたは許可を提供し、または特定の装置または特定の装置のプール（pool）（例えば、装置の集合）を提供するメカニズムを提供するものとしてその手法を一般化することができる。よって、ポート単位で単純にシステムコールを制限するのではなく、ポート（またはポートのプール）のいずれかにおいてシステムコールを行うことが許されまたは許されない特定のホストシステム（またはホストシステムのグループ）を示すことが十分である。加えて、そのような一般化したスキームを使用し、ホストシステムまたはホストシステムのグループの識別子に基づいて、メモリ位置（例えば、装置のプール）へのアクセスを選択的に割り当てることができる。

【0050】一般化されたシステムでは、システムコールは、要求元ID、アクセスタイプ、および対応する装置からなる。任意的に、パスワードを使用し、および／またはパスワードを要求元IDおよび／または要求元が属するグループに関連付けすることができる。要求元は、ホストコンピュータ、別のデータ記憶装置、またはデータ記憶装置へシステムコールを行うことができるあらゆるシステムとすることができる。アクセスタイプは、ディスクミラーリング、バックアップ、コピー、BCV処理、チェンジトラッカー（ChangeTracker）処理、その他などの要求されたアクセスのタイプを示すことができる。BCVおよびチェンジトラッカー処理はマサチューセッツ州ホプキントンのEMC社により提供され、ミラーされたボリュームの処理を含む。BCVは、ミラーボリュームとして開始し、次に独立に動作するように分割するボリュームに関連する。チェンジトラッカーは、各々への動作をトラッキングすることによる分割したボリュームの間の差をトラッキングすることに関連し、それにより1つのボリュームが別のものから復元されることが要求されるならば、変化したトラックのみが書き込みを要する。

【0051】いくつかの実施形態では、アクセス制御は読み書き動作の制御を含み、別の実施形態ではシステム管理コールのみが制御される。対応する装置は要求により影響を受ける装置を示すことができ、それにより例えば要求がディスクの読み取り動作を含む場合、その装置は読み取り動作の影響を受けるディスク（またはより大きなディスクスペースの一部）である。

【0052】図5を参照すると、マトリクス100は要求元のシステムQ、R、S、TおよびV（および、要求元のシステムのグループ化）を、装置W、X、Yおよび

Z（および、装置のプール）についてのアクセスレベルB、CおよびMに関連付けする情報を提供することを示す。いくつかの実施形態では、装置のプールは、図5に示す組み合わせIDに対向する唯一のIDを有することができる。

【0053】マトリクス100は、装置W、X、YおよびZ、ならびに装置のプールの種々の可能な組み合わせの列102、104、106、108および110を有する。システムは、マトリクス100に示す4個よりも多数または少数の装置を有することができ、代わりにマトリクス100は、要求しているユーザの組み合わせに対して許可レベルに関連付けしてリソースを許可するためのチャート、リスト、データベースまたはあらゆる他の手法の形態とすることができる。マトリクス100は、データ記憶装置22の一部である装置のアクセス要求を作るホストコンピュータまたは他の電氣的装置などの要求元システムQ、R、S、TおよびVに対応する行112、114、116、118および120を有する。要求元の数はいかなる数とすることができる。

【0054】要求元のグループ化は、要求元とアクセスされた装置の正しい組み合わせを見つけるために行わなければならないサーチの量を減少させることにより、改善されたアクセス速度を提供するようにシステムアドミニストレータにより行うことができる。例えば、ワークグループの全メンバーが、個別アクセスIDナンバーの一部としてワークグループナンバーを含む、割り当てられた個別アクセスIDナンバーを有することができる。こうして、ワークグループの全メンバーへアクセス可能なメモリ要素に個人がアクセスしている場合、グループIDナンバーはより迅速なデータベースのサーチを可能とする。要求元の識別のためにパスワードが使用される例では、IDナンバーが割り当てられるのと同様の方法でパスワードを要求元に割り当て、および／またはグループに割り当てることができ、パスワード自体を使用し、またはIDナンバーとの組み合わせにおいてパスワードを使用してアクセスを制御することができる。

【0055】いくつかのシステムは、有効なアクセスID（および／またはパスワード）を含まないアクセス要求に対してデフォルトアクセスID（および／またはデフォルトパスワード）を割り当てることにより、上述の実施形態にしたがって処理することができることに留意すべきである。マトリクス100では、デフォルトIDは行118の要求元Vにより示される。要求元Vは、列106の装置XへのBタイプアクセスを除いて、いずれの装置への許容されたアクセスも有しないことに留意すべきである。装置Xは例えば、インターネット接続を有する何者かにより使用されることが意図されているパブリックライブラリデータベースを示す。そのようなオープンアクセスについて、多数の他の潜在的な使用が想像できる。

【0056】一方、行114の要求元Qは、例示したマトリクスの装置プールの全メンバーへの完全なアクセスを有するようである。要求元QはシステムアドミニストレータのIDを示し、よって制御および構成の目的で、全てのメモリ要素への無制限アクセスを許容される必要がある。2つの記述されたケースの間には、無制限な数の可能な組み合わせが存在しうる。上述の実施形態にしたがって、例示した3レベルより多数の潜在的アクセスレベルが可能であることに留意すべきである。また、個々の要求元に対して装置（装置のプール）への特定のアクセスレベルを与えることは、個々の要求元のみを含むグループを形成することにより実現することができることに留意すべきである。

【0057】行112の4つの要求元（Q、R、SおよびT）のグループは、装置プール102～110の各々において、異なるグループのメンバーとしていくつかの個々の要求元が有するより少ない許容アクセスを有するように示されている。この例では、要求元Vは行112の要求元グループの一部ではないので、デフォルト値Vを含む行118は関心がない。行120では、要求元Sは装置プール列102で許容されたBおよびCアクセスを有し、それは本例ではW、X、YおよびZで示される4つの装置全てを含む。こうして、要求元グループRおよびS、行116は典型的にはBおよびCアクセス以上は許容されず、本例では許容されるアクセスを有しない。これは、要求元Rが例えばメモリ要素WおよびZに対応する装置に含まれるデータベースへのアクセスのみを許容された場合にそうなる。さらに、行112の4つの要求元のグループ化は、サブセットのグループ化に許容されるより大きなアクセスを許容してはならず、よって行112のグループは列102の装置プールに対するアクセスを有しないように図示されている。

【0058】図5からのQなどの要求元が全てのメモリ装置および装置のプールへの多数のアクセスを有する状況の例は、パスワードを紛失または忘れた時にパスワードをリセットすることができるメモリシステムアドミニストレータが、メインテナンスまたはサービスのためにあらゆるアクセス制御設定をオーバーライドし、新しいディスクなどの新しいメモリ装置を追加し、または装置プールから古いモデルを除去することを可能とし、装置プールのメンバーシップを再構成して変化するメモリ要求に順応し、新たなメモリ装置プールを作って拡張したカスタマベースを可能とし、または、システムアドミニストレータが提供するあらゆる他の機能を提供することを含むことができる。また、アドミニストレータはメンバーシップと要求元グループ数を再構成して装置プールへのアクセス制御速度を改善し、または許容されたアクセスの新たなレベルを規定し、または新たに許容されたタイプのシステムコールを適当に全てのデータ記憶装置に付加することができる。

【0059】装置および装置のプールがメモリの部分に対応する場合、上述の状況は、データ記憶装置内での秘密のユーザデータの安全を保持しつつ、区分可能なデータ記憶装置への効率的かつ柔軟なメモリアccessを認可されたユーザに提供する能力に関連する。上述の認可システムは、潜在的に危険なメモリアccessおよび機能を均一な方法で拒絶および受容するメカニズムを提供し、アクセスの決定は、認可されるべきでないことが明らかになったメモリアccess実行の開始において可変システム時間が無駄遣いされる前に行うことができる。

【0060】認可コード（および／またはパスワード）は、個別のホストコンピュータまたは他の要求元ベースで、またはグループアクセスベースで、または図5のマトリクスに示すような組み合わせベースで 사용할ことができる。その方法が潜在的な要求元毎のIDに制限される場合、認可マトリクスは大きく、要求元IDを見つけることは要求元がグループ化されている場合より長い時間を要する。一方、アクセスID番号を要求元の大きなグループに制限することは、要求元グループの種々のメンバーへ最適なアクセス可能性を割り当てる柔軟性を制限する。こうして、記載された実施形態は、各個別要求元についてのアクセスIDナンバーを提供して最大の柔軟性を提供し、グループアクセス値を装置プールアクセス値とマッチングすることによりアクセス認可速度を増加させるように働くグループIDナンバーを提供する。別の実施形態では、アクセスID番号はグループのみに割り当てられ、個別要求元には割り当てされない。2つのアクセスマトリクス方法を使用して最大の柔軟性と改善された認可速度を提供することができ、そこで第1のマトリクス（または、先に記載した他の認可方法）が要求元グループIDと装置プールIDを調べる。個別要求元が属するグループ全体が、要求されたタイプのアクセスに向けられた特定の装置プールの各メンバー毎の認可アクセスを有すれば、それ以上見る必要はない。これは、要求元グループIDがグループの最低メンバーと同程度のみ許容され、装置プールが最も制限されたプールのメンバーと同程度にのみ許容される場合にそうである。上述の状況に続くアクセスマトリクスの例は上述のように図5に示される。よって、記載されたアクセス制御方法は装置プールの変化レベルを支持することができ、アクセスの各レベルはアクセス動作の特定のレベルまたは組み合わせに対応する。さらに、上述の方法は、デフォルトアクセスIDを使用すること、および通信ポートなどの物理的メモリ構造が装置プールIDナンバーを有することを許容することにより、システムコールなどの危険な装置アクセス動作を妨げる既存の方法と両立しうる。

【0061】図5を参照して記載された実施形態は、1つの要求元グループを超える要求元を有する形態を含む。ホストが一部である各要求元グループについて個別

ホストコンピュータに唯一の要求元IDを割り当てることができる。その代わりに、唯一のIDはグループIDと個別IDナンバーとの組み合わせから構成することができる。組み合わせIDナンバーは先に述べた2段マトリクスアクセス認可方法を利用する。また、いずれにしても、IDの代わりにまたはその補助として、パスワードを使用することができる。

【0062】データ記憶装置のアクセス制御のための例示的構成は、IDナンバーシステム（および/またはパスワードシステム）を使用可能および不能とする命令を含み、ホストシステムおよび他の要求元についてのデフォルトおよび初期アクセスレベル、指定したIDナンバーの部分的に管理者のようなアクセスを認めるシステムアドミニストレータパスワード、所定時間量にわたって特定の要求元IDへのアクセスを否定する一時的オーバーライドコマンド、および所定時間量にわたって特定のIDへの完全なアクセスを与える一時的オーバーライドコマンドを規定することができる。これらのコマンドの使用は、パスワードを使用してシステムに入るシステムアドミニストレータに限定することができる。

【0063】図6を参照すると、フローチャート200はステップ202で開始する処理を示し、ステップ202では、ホストコンピュータまたは別のメモリシステムなどのあらゆるタイプの電子機器とすることができ、データ記憶装置へのアクセスを有する要求元システムは特定の装置または装置のプールへのアクセスの要求、例えばメモリの読み書きの要求を行い、または要求コピー、ミラーデータ、BCV動作、チェンジトラッカー動作、またはバックアップデータなどのシステムコールを行う。システムコールは、ホストコンピュータシステムから直接来ることができ、またはミラーリング要求の場合と同様に別のデータ記憶装置によりリレーすることができる。いくつかの実施形態では、システムコールのみが支持され、直接的読み書き動作はここに記載されるナンバー上では処理されない。

【0064】ステップ202の次はステップ204であり、そこではシステムコール要求を作るホストシステムのID（ホストシステムが属するグループのID）を、拒絶オーバーライド設定に対してチェックして拒絶オーバーライドが設定されているか否かを決定する。オーバーライド設定はメモリのオーバーライド位置に変数として記憶することができる。設定された拒絶オーバーライドは、IDおよび対応する装置についてのアクセス設定にかかわらずシステムコールが否定されることを示す。そのような拒絶オーバーライド設定は、システム故障などの多数の起こりうる理由についてシステムアドミニストレータにより設定でき、オーバーライドが設定されてから固定時間後にオーバーライド状態をオーバーライドが無い状態に戻すためのタイマー設定がありうる。ステップ204で拒絶オーバーライドが設定されていると決

定されると、その要求はデータ記憶装置によっては許可されず、データ記憶装置はアクセス否定メッセージをステップ222で要求元システムに送ることができ、要求プロセスはステップ210で終了する。

【0065】ステップ204で拒絶システムコールオーバーライドが設定されていないことが決定されると、ステップ212でバスオーバーライド設定（メモリのオーバーライド位置に記憶し、または他の位置に記憶可能である）がチェックされる。バスオーバーライドは、要求元および対応する装置のアクセス設定にかかわらずシステムコールが許可されることを示す。バスオーバーライドが設定されると、記憶システムはステップ214でシステムコールを完了し、プロセスはステップ210で終了する。任意的に、システムコールアクセスが許可され、完了したことを示すメッセージを、要求しているシステムに送信することができる。

【0066】バスオーバーライドが設定されていないならば、ステップ216でコール要求を調べて、アクセスIDナンバーが要求中に含まれているか否かを決定する。データ記憶装置に接続したユーザシステムの全てがアクセスIDナンバーを有するわけではない。アクセスIDは要求元IDと同一とすることができ、または異なる唯一のナンバーとすることができ、もしくは要求元が属するグループのIDとすることができ、いくつかの例では、より新しいシステム（すなわち、IDまたはグループID）の能力を有しないより古いシステムを依然として使用することができ、よってシステムの有用性を拡張するとともに新製品の導入を容易にする逆行した互換性を提供する。また、アクセスIDの代わりに、または補助的に、パスワードを使用することができることを述べておく。要求中に正しいアクセスIDが見つかり、制御はステップ220へ進む。アクセスIDが見つからないと、ステップ218でデフォルトIDが割り当てられ、制御はステップ220へ進んで、アクセスIDをチェックしてアクセスIDが有効であるか否かを決定する。アクセスIDナンバーが許可可能なアクセスIDナンバーのテーブル中に見つからない場合、制御はステップ222へ進み、システムコールアクセス否定メッセージを要求元のシステムへ送信することができ、プロセスはステップ210で終了する。

【0067】アクセスIDがデータ記憶装置により適合されると、ステップ224でアクセス要求のタイプをチェックして要求された特定のタイプのシステムコールが許可されるか否かを決定する。実行されている要求のタイプが対応する装置（装置プール）について許可されていないと、制御はステップ222へ進み、システムコールアクセス否定メッセージを要求元のシステムへ送信することができ、次に処理はステップ210で終了する。

【0068】要求のタイプが一般的に許可されると、アクセスIDがステップ226でチェックされ、特定の要

元（要求元が属するグループ）が対応する装置（装置プール）に関して要求された特定のタイプのシステムコールを許可されたか否かを確認する。否定的であれば、制御はステップ222へ進み、要求元のシステムにシステムコールアクセス否定メッセージを送信することができ、次に処理はステップ210で終了する。IDが、実行されたタイプのコールの一般的な使用を許可されると、制御はステップ228へ進み、そこでシステムコールにより影響を受ける装置をチェックして対応する装置プールが要求されたタイプのアクセスを許可するか否かをチェックする。要求されたタイプのアクセスが許可されないと、制御はステップ222へ進み、そこで要求元のシステムへシステムコールアクセス否定メッセージを送信することができ、次に処理はステップ210で終了する。

【0069】装置プールが要求されたタイプのアクセスを許可する場合、ステップ230で要求されたアクセスが許可されるか否かが決定される。これは、データ記憶装置のメモリ空間の一部または複数部分などの装置プールへの特定のアクセスを割り当てられた要求元に要求が制限される状況を維持することを助ける。IDが装置プールへの適当なアクセスを有しない場合、制御はステップ222へ進み、そこで要求元のシステムへシステムコールアクセスメッセージを送信することができ、アクセスプロセスはステップ210で終了する。アクセスIDナンバー、装置プールIDナンバーおよび要求されたアクセスのタイプが一致すれば、ステップ214でシステムコールが完了し、次にアクセスプロセスはステップ210で終了する。

【0070】図6のフローチャートについてのコードは、図3に示され、先に説明したのと類似したスキームを使用して実施することができる。すなわち、セキュリティモジュール（図3のモジュール64に類似する）は図6に示すステップを実行する。ユーザのどのグループがどのプールへどのタイプのアクセスを有するかを示すセキュリティデータを従来の方で集中して、ここに記載する機能を提供することができる。オーバーライド設定はオーバーライドメモリ位置に記憶することができる。図6のフローチャートを実施するための他の手法は従来技術の当業者に自明である。

【0071】ここに記載するシステムは、システムコール要求を作成するユーザ（および／またはユーザが属するグループのID）、その要求中のどの装置プールが関連するか、どのタイプの要求がなされているか、および、その要求を許可するようにシステムが構成されているかを決定する。装置プールは、分離した物理的ディスク、ディスクのグループ、または大きなディスクの部分に分割されるメモリシステムの部分とすることができる。メモリリソースは、許可されたシステムコールのタイプについて、およびどの特定の要求元（または要求元

のグループ）がメモリへのアクセスを許可されているかについて同一の要求を有するメモリプールにグループ化することができる。例えば、プールXは20個のディスクシステムを有することができ、企業Aからの要求元に対してのみ許可されたアクセスを有することができる。プールYは大きな磁気ディスクの一部を含むことができ、企業AおよびBによるアクセスを許可するが、システムアドミニストレータ以外の者からのミラーリング要求を許可しない。記述される実施形態はIDナンバーに基づくアクセスを許可するので、複数の人間のユーザを伴う単一の大型コンピュータに多数の異なるアクセスIDナンバーを与え、それにより異なる各ユーザ（および／またはユーザのグループ）が記憶装置の異なる部分への異なるレベルのアクセスを有するようにする。これは、単一の企業内の異なる部門が、異なる部門によりデータベース内の値を変更されることを防止したいと考え、またはその部門が許可されるより多くのメモリ空間を使用することを防止したいと考える時に有用である。ここに記載される実施形態は、要求元IDナンバー（グループIDナンバー）を使用して記憶アクセスおよびアクセスのタイプを決定し、そうして要求元が接続されているメモリポートに依存してアクセスを制御するような物理的調整手段を使用するよりも、論理的装置調整器を構成する。ここに記載されるように、IDの代わりに、またはそれに加えて、パスワードを使用することができる。

【0072】アクセスIDナンバーを生成し、それらをデータ記憶装置に登録するステップの例は、ホストコンピュータシステム（または他の要求元システムタイプ）のアドミニストレータが、ホストコンピュータシステムの唯一のハードウェアID、ホストコンピュータシステムが属するグループのID、ホストシステムについてのパスワード、ホストシステムが属するグループのパスワード、および／またはファイバーチャネルワールドワイドネームを取得するためのユーティリティプログラムを起動し、またホストシステムについて複数のアクセスIDナンバーの要求が存在するかを決定することを含む。ホストアドミニストレータは、ハードウェアID（またはパスワードまたはファイバーチャネルワールドワイドネーム）およびホストによりシステムアドミニストレータに対して使用されるネームおよびオペレーティングシステムを供給する。複数の個別ユーザがホストシステムに関連し、各々が異なるレベルのアクセスを必要とする場合、個別のパスワードまたはIDナンバーを各ユーザに割り当てることができる。これらをホストシステムIDナンバーと組み合わせて、依然としてホストシステム情報を提供可能な各ユーザのための唯一のIDナンバーを生成することができる。ユーザをグループ化することができ、IDナンバーを各グループに提供することができる。

【0073】付加的なセキュリティについて、メモリアドミニストレータが安全なハッシュプログラムとして知られるものを通じてIDナンバーを実行することにより、IDナンバーをさらにランダム化し、この場合アクセスIDナンバーと呼ばれる唯一のIDナンバーを生成することができる。異なるハードウェア装置が同一のIDナンバーを有する例では、付加的な、おそらくランダムなデータを安全なハッシュ関数への入力として使用することによりアクセスIDナンバーを生成することができる。データ記憶装置は、アクセスIDを記憶し、それをメモリ要素などの選択された装置プールに関連付ける。メモリ要素は、ディスクまたはディスクの一部などの単一の要素、もしくはメモリ要素のグループのいずれかとすることができる。アクセスが特定の装置プールと関連付けされると、システムアドミニストレータはアクセスレベルを割り当てまたは除去する。安全なハッシュプログラムのこの例示的实施形態における使用により、アクセスIDナンバーはホストシステムによっても知ることができないが、アクセス時にハードウェアIDから再生成され、よって認可されたホストシステムとは異なる位置からのあらゆるアクセスを防止する。

【0074】図7を参照すると、線図250は別の実施形態を示し、そこではセキュリティデータを別の方法で記憶することができる。線図250は、リンクされたリストとして記憶された複数のノード252～254を示す。ノード252～254の各々はユーザ又はユーザのグループに対応することができる。よって、ここでの説明では、「ユーザ」の語はユーザのグループの同義語と考えることができ、これ以外の他の部分における説明と一致する。

【0075】各ユーザについて、それに関連付けられた許容可能な複数のアクションが存在し、それにより、例えばノード252に対応するユーザはノード252に接続された複数のノード256～258に対応するアクションを実行することができる。同様に、ノード253に対応するユーザは複数の接続されたノード262～264に対応するアクションを実行することが許容され、ノード254に対応するユーザは複数の接続されたノード266～268に対応するアクションを実行することが許容される。各アクションは1つ以上の装置に関連付けることができ、またはいくつかの例ではアクションは関連する装置を有しない。アクションに対応する各ノード256～258、262～264、266～268は、許容される装置に対応する関連付けされたノードのリストを有する。よって、例えばノード256に対応するアクションはそれに接続されたリスト272を有し、リスト272は、ノード256に対応するアクション及びノード252に対応するユーザについて受け入れ可能な装置に対応するノードを含む。同様に、ノード257はそれに接続されたリスト274を有し、ノード2

58はそれに接続されたリスト276を有する。他の装置のリスト282、284、286、292、294、296も図示されている。

【0076】ユーザノード252～254はあらゆる数のユーザを示す。すなわち、線図250に示す3つのノード252～254ではなく、あらゆる数のユーザ及びあらゆる数のノードが存在しうる。同様に、各ユーザに関連付けされたあらゆる数のアクション、及び各アクションに関連付けされたあらゆる数の装置が存在しうる。さらに、いくつかの実施形態では、以下に詳細に説明するように、1つ以上のユーザノード252～254がデフォルトユーザを示すことができる。

【0077】ユーザ252に接続されたノード256～258などのアクションノードは、ユーザが実行可能な種々のアクションを示す。よって、ノード252に対応するユーザは、それに接続された各ノード256～258に対応するアクションを実行することができる。すなわち、ノード256～258を有するリンクされたリストは、ノード252に対応するユーザに認められた各アクションのエントリーを含む。

【0078】アクションノードリスト中の各アクションについて、アクションを実行することができる許可可能な装置のリストが存在する。よって、例えばノード256について、リスト272中のノードは、ノード252に対応するユーザについて実行可能であるノード256に対応するアクションとの関係でどの装置を使用できるかを示す。いくつかのアクションについては、装置に対応するリンクリストはヌル(null)（すなわち、エントリーを含まない）とすることができることを述べておく。これは、例えばユーザIDを要求するシステムコールのように、特定の装置上において実行されるのではないアクションについて生じる。さらに、以下の詳細に説明するように、いずれかの装置に対応しまたは対応しないユーザ規定アクションをユーザが作ることが可能である。よって、データ記憶装置22が実行可能しうるアクションについて、ユーザはまず望ましいアクションが認められるか否かを決定するための要求をすることができる。次に、アクションが認められると、ユーザはデータ記憶装置22がそのアクションを実行することを要求することができる。その代わりに、データ記憶装置22が実行不可能なアクションについて、ユーザは単に認可要求ステップのみを実行することができる。

【0079】実際には、1つ以上の特定の装置（または場合によっては0個の装置）を使用して特定のアクションが実行可能か否かを要求した時、ユーザノード252～254を最初にスキャンし、要求しているユーザに対応するノードを見つける。適合しているノードが見つかり、次にアクションに対応するノードを含む接続リストをレビューして、要求されているアクションが要求しているユーザに対して許容されるか否かを決定する。そ

のアクションが許容されることが決定されると、次にそのアクションが特定の装置を必要とするものであるか否か、次にアクションに対応するノードに接続された装置に対応するリストをスキャンして、そのユーザのアクションと関連して要求された装置が許容されるか否かを決定する。

【0080】いくつかの実施形態では、ユーザが規定可能なアクションを使用して、データ記憶装置22上でまたはデータ記憶装置22により実行することができないアクションについて許可（すなわち許可されたか否定されたか）を返すシステムを作ることができる。その場合、ユーザは単純に種々のユーザについての特定の許可を伴って特定のユーザ規定可能アクションを規定することができる。次に、ユーザ規定可能アクションは特定のアクションに対応する1つ以上のリストに添付することができる。次に、ユーザは特定のアクションについての許可を要求し、その特定のアクションが許可されたか否定されたかを示す表示を受信することができる。もちろん、そのアクションがデータ記憶装置22の動作に対応しないならば、ユーザはデータ記憶装置22がそのアクションを実行する要求を追求することはできないであろう。しかし、いくつかの例では、許可または否定されたアクセス情報を単に受信することが有益であろう。

【0081】線図250に示されたデータは、チャート、リスト、複数のリンクされたリスト、アレイ、およびデータベースを含む種々のデータ記憶手法の1つで記憶することができることを述べておく。さらに、線図250に示されるデータを図3のセキュリティ構成データ要素66に記憶することもできる。

【0082】図8を参照すると、フローチャート300は図7の線図250に示すデータを使用するシステムの動作を示す。フローチャート300は、任意的に装置を伴う、アクションの許可のユーザ要求の処理を示す。

【0083】処理は第1ステップ302で開始し、ここでは要求しているユーザがユーザリストのノードに対応するか否かが決定される。対応しない場合、制御はステップ302からステップ304へ進み、デフォルトユーザに対応するノードが使用される。いくつかの実施形態では、デフォルトユーザは、具体的にリストされていないユーザについて使用される。デフォルトユーザはデフォルトアクション及びデフォルト装置に関連付けすることができる。

【0084】ステップ304に、またはユーザがリスト上のノードに対応することがわかった場合にはステップ302に続くのはテストステップ306であり、そこでは要求されたアクションが、ユーザに対応するノードに接続されたノードリスト上にあるか否かを決定する。否定的であれば、制御はステップ306からステップ308へ進み、要求が否定される。すなわち、要求されたアクションがユーザに対応するノードに接続されたノード

に対応しなければ、その要求はステップ308で否定される。要求を否定することは、その要求が否定されたことを示すコードを返信することを含む。

【0085】ステップ306で要求されたアクションが許可された（すなわち、適当なノードの1つに対応する）ことが決定されると、制御はステップ306からステップ310へ進み、要求されたアクションが装置を使用するか否かが決定される。上述のように、いくつかのアクションは装置を必要とせず、または使用しない。そのようなアクションは、例えばシンメトリクス（Symmetric）のIDを要求することを含む。テストステップ310で、要求されたアクションが装置を含まないことが決定されると、制御はステップ310からステップ312へ進み、その要求が許可されたことを示す表示がユーザへ返される。また、ステップ312が以下に詳細に説明するタグを返すことも可能である。

【0086】テストステップ310において、要求されたアクションが装置を使用することが決定された場合、制御はステップ310からテストステップ314へ進み、その装置がそのアクションについて許可されたリスト上にあるか否かが決定される。否定的である場合、制御はステップ314からステップ308へ進み、要求が否定される。そのかわりに、テストステップ314において装置がリスト上にあると決定されると、制御はステップ314からステップ312へ進み、要求が許可される。ステップ308またはステップ312に続いて、処理は終了する。

【0087】いくつかの実施形態では、デフォルトユーザは無くてもよい。その場合、ステップ304は実行されない。その代わりに、ステップ302において要求しているユーザがユーザのリスト上に無いことが決定されると、制御はステップ302からステップ308へ進み、要求が否定される。これは、フローチャート300上の代替的パス314により示されている。

【0088】いくつかの実施形態では、タグを利用して、その後の要求に関連して提出されるパスワードまたはキーをユーザに与えることができる。タグは、許可に成功した要求を行ったユーザに返信することができる。次に、ユーザは後に同一の動作を実行することに関してタグを使用することができるであろう。いくつかの実施形態では、タグの有効期間は満了せず、システムのセキュリティが変化した後でもユーザがアクションを実行することを許容し、そうでなければ要求された動作は許可されない。

【0089】図示および詳細に説明した好適な実施形態との関係で本発明を説明してきたが、従来技術の当業者には種々の変形および改良が容易にわかるであろう。したがって、本発明の精神および視野は請求の範囲によってのみ限定されるべきである。

【図面の簡単な説明】

【図 1】本発明にしたがって構成された記憶装置を示す概略図である。

【図 2】本発明にしたがって構成された複数の記憶装置を示す概略図である。

【図 3】本発明の実施形態の動作を示すデータフロー図である。

【図 4】本発明の実施形態にしたがって実行されるステップを示すフローチャートである。

【図 5】要求元と記憶要素と許容可能なシステムコールとの関連を示すテーブルである。

【図 6】本発明のユーザ論理装置の実施形態の動作を示

す論理的フローチャートである。

【図 7】本発明の実施形態にしたがう、セキュリティデータを記憶するためのデータ構造を示す図である。

【図 8】本発明の実施形態にしたがう、図 7 のデータへのアクセスを示すフローチャートである。

【符号の説明】

20 システム

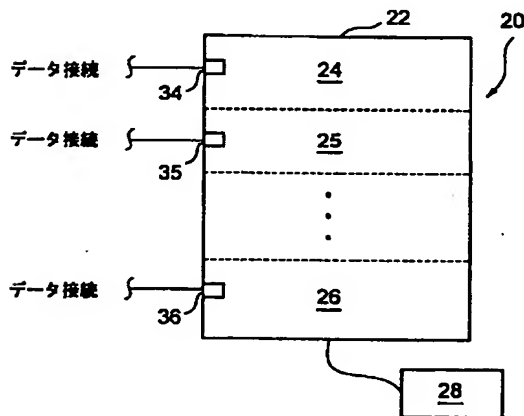
22 データ記憶装置

24、25、26 セクション

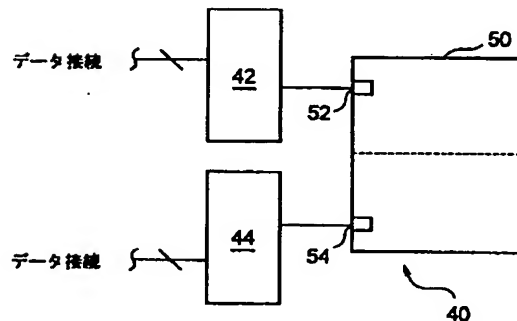
28 外部制御装置

34、35、36 外部ポート

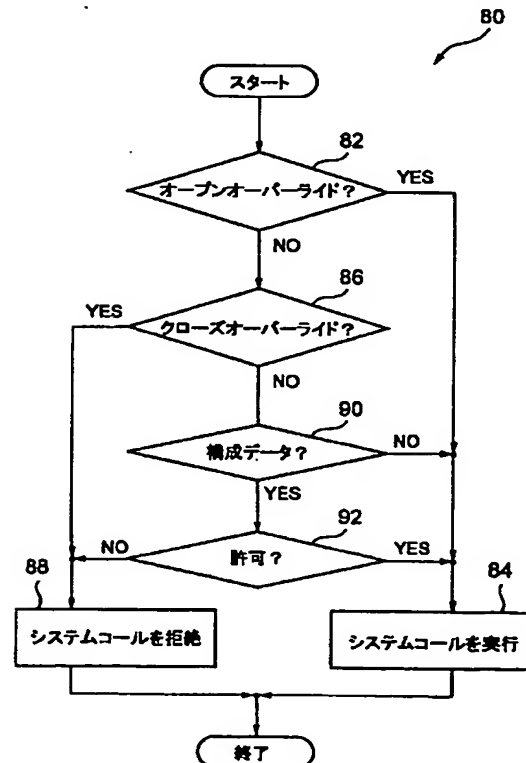
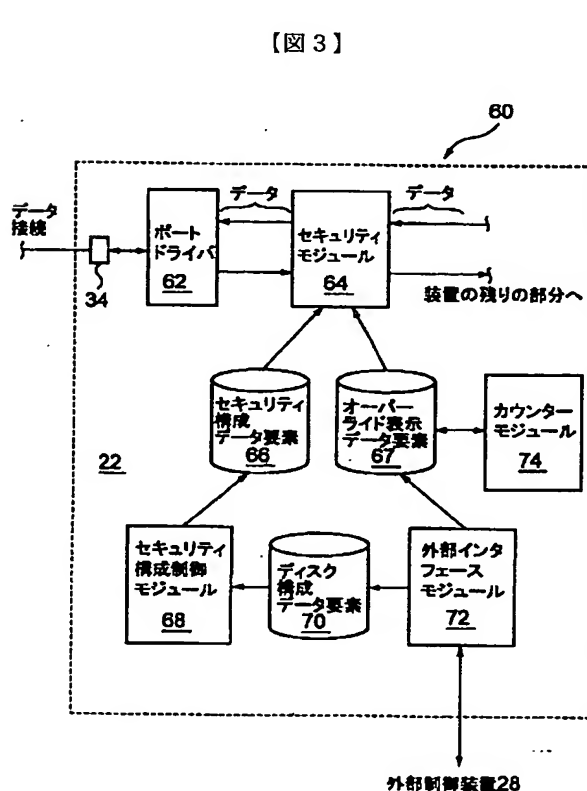
【図 1】



【図 2】



【図 4】

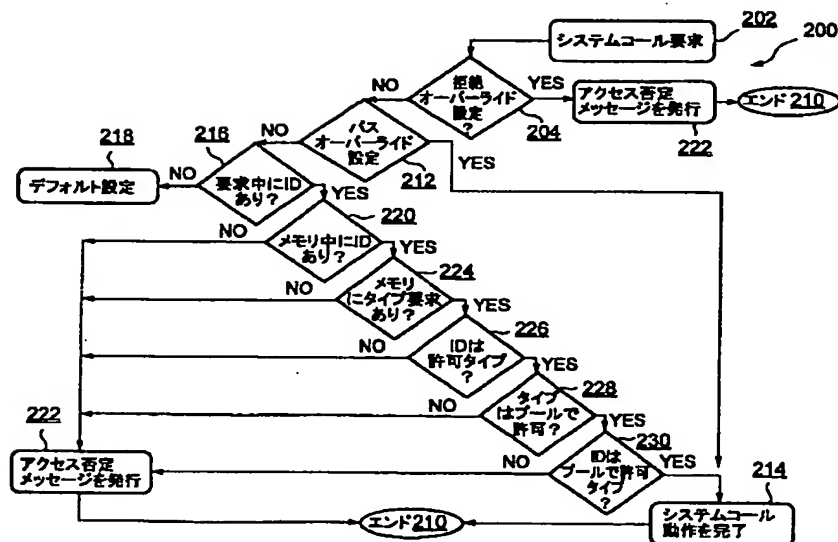


【図5】

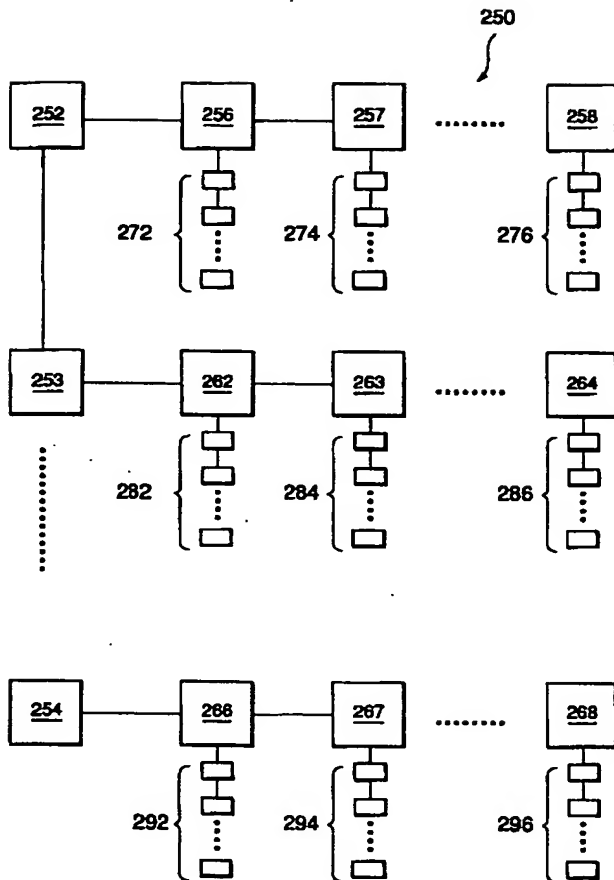
100

| 装置プール 要求元グループ | W,X,Y,Z | W | X | W,Z | X,Y | |
|------------------|---------|-------|-------|-------|-------|-----|
| Q,R S,T | NONE | B,C,M | B,C | B,M | NONE | 112 |
| Q | B,C,M | B,C,M | B,C,M | B,C,M | B,C,M | 114 |
| R,S | NONE | B,C,M | B,C | B,M | NONE | 116 |
| V | NONE | NONE | B | NONE | NONE | 118 |
| S | B,C | B,C,M | B,C | B,M | B,C,M | 120 |
| | 102 | 104 | 106 | 108 | 110 | |

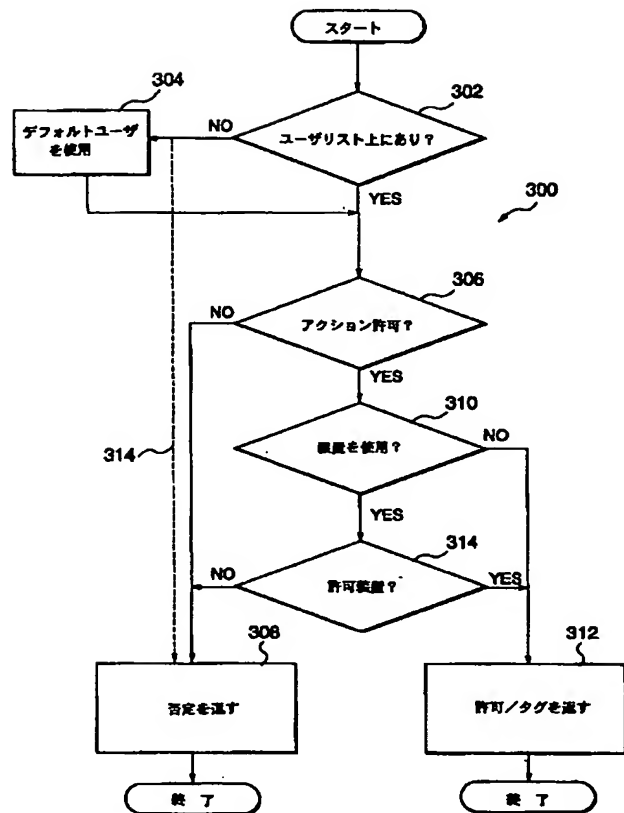
【図6】



【図7】



【図8】



フロントページの続き

(31) 優先権主張番号 09/774532
 (32) 優先日 平成13年1月31日(2001. 1. 31)
 (33) 優先権主張国 米国(US)
 (31) 優先権主張番号 特願2000-396584(P2000-396584)
 (32) 優先日 平成12年12月27日(2000. 12. 27)
 (33) 優先権主張国 日本(JP)
 (31) 優先権主張番号 特願2000-397854(P2000-397854)
 (32) 優先日 平成12年12月27日(2000. 12. 27)
 (33) 優先権主張国 日本(JP)

(72) 発明者 サシェ・ケイ・カナバシ
 アメリカ合衆国 マサチューセッツ
 01581 ウェストバラ ウィンザー リッ
 ジ ドライヴ 301
 (72) 発明者 ブライアン・ギャレット
 アメリカ合衆国 マサチューセッツ
 01748-1032 ホプキントン フルーツ
 ストリート 35

Fターム(参考) 5B017 AA07 BA06 BB06 CA07
 5B065 BA01 EA33 PA02 PA04 PA11
 PA12 PA20